CA ARCserve® Central Virtual Standby

Benutzerhandbuch

r16

Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden.

Diese Dokumentation darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden. Diese Dokumentation enthält vertrauliche und firmeneigene Informationen von CA und darf vom Nutzer nicht weitergegeben oder zu anderen Zwecken verwendet werden als zu denen, die (i) in einer separaten Vereinbarung zwischen dem Nutzer und CA über die Verwendung der CA-Software, auf die sich die Dokumentation bezieht, zugelassen sind, oder die (ii) in einer separaten Vertraulichkeitsvereinbarung zwischen dem Nutzer und CA festgehalten wurden.

Ungeachtet der oben genannten Bestimmungen ist der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2012 CA. Alle Rechte vorbehalten. Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber.

CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

CA Kontaktieren

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Support-Links für CA ARCserve Central Applications:

CA Support Online stellt eine Vielfalt an Ressourcen zur Lösung von technischen Problemen zur Verfügung und bietet einfachen Zugriff auf wichtige Produktinformationen. Mit CA Support haben Sie zu jeder Zeit schnellen und einfachen Zugang zu vertrauenswürdigen Auskünften. Über die folgenden Links gelangen Sie zu den unterschiedlichen CA Support-Seiten, die Ihnen zur Verfügung stehen:

- **Informationen zum Support**: Über diesen Link erhalten Sie Informationen zu Wartungsprogrammen und Support-Angeboten sowie zu Bedingungen, Rechtsansprüchen, Service Level Objectives (SLO) und Servicezeiten.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrierung für Support**: Dieser Link führt Sie zum CA Support Online-Registrierungsformular, mit dem Sie Ihren Produkt-Support aktivieren können.

  https://support.ca.com/prodinfo/supportregistration

- **Technischer Support**: Die folgende Verknüpfung führt Sie zur One-Stop Product Support-Seite für CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Änderungen in der Dokumentation

Das Dokument enthält Benutzer-Feedback, Verbesserungen, Korrekturen und andere kleinere Änderungen, um die Verwendung und das Produktverständnis oder die Dokumentation selbst zu verbessern.

Seit der GA-Version dieser Dokumentation wurden folgende Aktualisierungen der Dokumentation vorgenommen:

Aktualisierung 6

- Der Abschnitt Richtlinienbereitstellung (siehe Seite 40) wurde aktualisiert. Dieser Abschnitt enthält jetzt einen Hinweis darauf, dass der Richtlinienbereitstellungsstatus in der Knotenlistenansicht in der Richtlinienspalte abgelesen werden kann.
- Der Abschnitt Aktualisieren von Knoten (siehe Seite 51) wurde aktualisiert. Das Thema beschreibt, wie Sie gleichzeitig mehrere Knoten aktualisieren können, sei es mithilfe der vorhandenen Anmeldeinformationen oder indem Sie neue Anmeldeinformationen angeben. Sie können auch den Server zwingen, die ausgewählten Knoten zu verwalten.
- Der Abschnitt Knotengruppen hinzufügen (siehe Seite 29) wurde aktualisiert. Dieser Abschnitt ersetzt die "nicht zugewiesene" Knotengruppe durch "Knoten ohne Richtlinie" und die "nicht gruppierte" Knotengruppe durch "Knoten ohne Gruppe".
- Der Abschnitt Einschalten von virtuellen Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots (siehe Seite 90) wurde aktualisiert. Der aktualisierte Abschnitt behandelt eine neue Schaltfläche namens "Standby-VM" in der Knotenaktions-Symbolleiste. Diese Funktion ermöglicht es Ihnen, einen virtuellen Rechner direkt aus der Anwendung heraus einzuschalten.

Aktualisierung 5

- Das Dokument wurde mit Benutzer-Feedback, Verbesserungen, Korrekturen und anderen kleineren Änderungen aktualisiert, um die Verwendung und das Produktverständnis oder die Dokumentation selbst zu verbessern.
- Hinzufügen von Knotengruppen (siehe Seite 29). Dieses Thema wurde aktualisiert, um die Filter "Gruppe" und "Knotenname" hinzuzufügen.
- Zuweisen von Knoten zu Richtlinien (siehe Seite 39). Dieses Thema wurde aktualisiert, um die Filter "Gruppe" und "Knotenname" hinzuzufügen.
- Aktualisieren von Knoten (siehe Seite 51). Dieses Thema wurde aktualisiert, um verschiedene Methoden einzuschließen, wie mehrere Knoten aktualisiert werden können.
- Zuweisung von Knoten zu Richtlinien aufheben (siehe Seite 67). Dieses Thema wurde aktualisiert, um die Filter "Gruppe" und "Knotenname" hinzuzufügen.

Aktualisierung 4

- Der Abschnitt Bereitstellen von Richtlinien (siehe Seite 40) wurde aktualisiert und mit weiteren Informationen ergänzt, die beschreiben, wie sich der Bereitstellungsvorgang auf Knoten auswirkt, die Sie aus Host-Based VM Backup importieren.
- Es wurde das Thema "Unterbrechen und Wiederaufnehmen von Heartbeat-Signalen" aktualisiert, um zu beschreiben, wie Sie Heartbeat-Signale vom Virtual Standby-Server (siehe Seite 84) und direkt vom Knoten aus (siehe Seite 86) unterbrechen und wiederaufnehmen.
- Das Aussetzen und Wiederaufnehmen von Virtual Standby-Jobs wurde aktualisiert, um zu beschreiben, wie Virtual Standby-Jobs vom Virtual Standby-Server (siehe Seite 87) und direkt vom Knoten aus (siehe Seite 88) unterbrochen und wiederaufgenommen werden.
- Es wurden die Themen "Wiederherstellen von Daten aus CA ARCserve D2D-Wiederherstellungspunkten" (siehe Seite 107), "Wiederherstellen von Daten aus CA ARCserve D2D-Dateikopien" (siehe Seite 112), "Wiederherstellen von Daten mithilfe von "Wiederherzustellende Dateien/Ordner suchen"" (siehe Seite 117) und "Wiederherstellen von Microsoft Exchange-E-Mail-Nachrichten" (siehe Seite 169) aktualisiert. Diese Themen beschreiben, wie Daten mithilfe der neuen Aktion "Wiederherstellen" auf der Symbolleiste wiederhergestellt werden.
- Das Thema "Ändern des Server-Kommunikationsprotokolls" (siehe Seite 178) wurde hinzugefügt. Dieses Thema beschreibt, wie das von den CA ARCserve Central Applications-Komponenten verwendete Kommunikationsprotokoll mithilfe einer Batch-Datei von HTTP in HTTPS und von HTTPS in HTTP geändert wird.

Inhalt

Kapitel 1: Einführung in CA ARCserve Central Virtual Standby 11

Einführung 11
Funktionsweise von CA ARCserve Central Virtual Standby 12
CA ARCserve Central Applications-Bookshelf 14

Kapitel 2: Installation von CA ARCserve Central Virtual Standby 15

Erforderliche Installationsaufgaben 15
Installationshinweise 17
Installation von CA ARCserve Central Virtual Standby 18
Deinstallieren von CA ARCserve Central Virtual Standby 20
CA ARCserve Central Virtual Standby automatisch installieren 20
CA ARCserve Central Virtual Standby automatisch deinstallieren 23

Kapitel 3: Erste Schritte mit CA ARCserve Central Virtual Standby 25

Stellen Sie sicher, dass der CA ARCserve Central Virtual Standby-Server mit den Knoten kommunizieren kann. 26
Anmeldung bei CA ARCserve Central Virtual Standby 27
Hinzufügen von Knoten nach IP-Adresse oder Knotennamen 28
Hinzufügen von Knotengruppen 29
Geben Sie das ESX Server- oder vCenter Server-System für VMware-basierte Knoten an 30
Erstellen von Richtlinien 32
Zuweisen von Knoten zu Richtlinien 39
Bereitstellen von Richtlinien 40

Kapitel 4: Verwenden von CA ARCserve Central Virtual Standby 43

Anmelden bei CA ARCserve D2D-Knoten 43
Anmelden an Überwachungsservern 44
Aufgaben zur Wartung von Knoten 45
- Importieren von Knoten aus einer Datei 46
- Hinzufügen von Knoten von CA ARCserve Central Host-Based VM Backup-Servern 48
- Aktualisieren von Knoten 51
- Löschen von Knoten 52
- Freigeben von Lizenzen von Knoten 53
- Überwachen von Knoten über den Überwachungsserver beenden 55

Aktualisieren von Knoten und Richtlinien nach einer Änderung des Hostnamens des CA ARCserve Central Applications-Servers 56
Aufgaben zur Verwaltung von Knotengruppen 56
Ändern von Knotengruppen 57
Löschen von Knotengruppen 58
Filtern von Knotengruppen 59
Verwaltungsaufgaben zu Virtual Standby-Richtlinien 59
Bearbeiten oder Kopieren von Richtlinien 60
Zuweisung von Knoten zu Richtlinien aufheben 67
Löschen von Richtlinien 68
Konfigurationsaufgaben der Anwendung 69
Konfigurieren der E-Mail-Einstellungen 69
Konfigurieren automatischer Updates 70
Konfigurieren von Voreinstellungen für Social Networking 73
Ändern des Administratorkontos 74
Anzeigen von Protokollen 76
Links zur Navigationsleiste hinzufügen 77
Startseite von Virtual Standby 78
So verwenden Sie den Bildschirm "Übersicht über Virtual Standby" 78
So verwenden Sie die Serverliste 79
Anzeigen von "Zusammenfassende Informationen" zum neuesten Virtual Standby-Job 80
Überwachen des Status von virtuellen Konvertierungsjobs 81
Anzeigen der Virtual Standby-Einstellungen für Quellserver 82
Anzeigen der Liste der Wiederherstellungspunkt-Snapshots 83
CA ARCserve Central Virtual Standby-Überwachungs-Aufgaben 83
Unterbrechen und Wiederaufnehmen von Heartbeat-Signalen des Virtual Standby-Servers 84
Unterbrechen und Wiederaufnehmen von Virtual Standby-Jobs vom Virtual Standby-Server aus 87
Einschalten von virtuellen Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots 90
Anzeigen von Aktivitätsprotokolldaten über Jobs 94
Anzeigen von Statusinformationen zu Virtual Standby-Jobs vom Virtual Standby-Server aus 97
Anzeigen von Informationen über zu CA ARCserve D2D-Knoten zugewiesenen Richtlinien 100
So schützen Sie virtuelle Virtual Standby-Rechner 105
Wiederherstellen von Daten aus CA ARCserve D2D-Wiederherstellungspunkten 107
Wiederherstellen von Daten aus CA ARCserve D2D-Dateikopien 112
Wiederherstellen von Daten mithilfe von "Wiederherzustellende Dateien/Ordner suchen" 117
Wiederherstellen von Quellservern mithilfe von Bare-Metal-Recovery 122
Wiederherstellen von Quellservern mithilfe von CA ARCserve D2D-Sicherungsdaten 124
Wiederherstellen von Quellservern mithilfe von Daten aus Hyper-V-basierten virtuellen Virtual Standby-Rechnern 139
Wiederherstellen von Quellservern mithilfe von Daten aus VMware-basierten virtuellen Virtual Standby-Rechnern 153
Wiederherstellen von Microsoft Exchange-E-Mail-Nachrichten 169

Ändern des Server-Kommunikationsprotokolls 178

Kapitel 5: Fehlerbehebung in CA ARCserve Central Virtual Standby 181

Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist. 182
Leere Webseiten oder JavaScript-Fehler treten auf 184
Beheben von Problemen beim Laden von Seiten 186
Bei der Anmeldung in CA ARCserve D2D-Knoten und -Überwachungsserver werden Webseiten nicht richtig geladen 187
Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift. 188
CA ARCserve D2D-Webservice schlägt auf CA ARCserve D2D-Knoten fehl 189
Der CA ARCserve D2D-Webservice wird nur langsam ausgeführt. 192
CA ARCserve Central Virtual Standby kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen. 194
Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt. 195
Beim Hinzufügen von Knoten werden ungültige Anmeldeinformationen angezeigt. 196
Meldungen zu ungültigen Anmeldeinformationen unter Windows XP 197
Fehler wegen verweigerten Zugriffs beim Hinzufügen eines Knotens nach IP/Namen 198
Knoten werden nach einer Namensänderung nicht mehr im Bildschirm "Knoten" angezeigt 200
Fehler "Operating System Not Found" treten auf 201
Virtual Standby-Jobs an Hyper-V-Systeme schlagen fehl 202
Virtual Standby-Jobs schlagen aufgrund interner Fehler fehl 202
Virtual Standby-Jobs im Hotadd-Transportmodus schlagen fehl 205
Virtual Standby-Jobs enden Mit Warnmeldungen zu fehlenden Sitzungen 207
Sicherungs- und Wiederherstellungsjobs verwenden den SAN-Transportmodus nicht 208
Bei Sicherungen und Wiederherstellungen im Hotadd-Transportmodus werden Datenträger nicht geladen 210
Fehlernummern der Fehlerbehebung 211
Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet 212
Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer 8 und 9 nicht ordnungsgemäß geöffnet 215
Bei der Verwendung einer japanischen Tastatur können in Filterfeldern keine Sternchen und Unterstriche als ein Platzhalter verwendet werden 216
Virtuelle Rechner nicht automatisch eingeschaltet 216

Kapitel 6: Best Practices 217

Auswirkungen des Installationsprozesses auf das Betriebssystem 217
- Binärdateien mit unrichtigen Informationen zur Dateiversion 219
- Binärdateien ohne eingebettetes Manifest 219
- Binärdateien mit "Require Administrator"-Berechtigungen im Manifest 220

Funktionsweise der CA ARCserve Central Virtual Standby-Lizenzierung 222

Terminologieglossar 225

Index 227

Kapitel 1: Einführung in CA ARCserve Central Virtual Standby

Dieses Kapitel enthält folgende Themen:

Einführung (siehe Seite 11)
Funktionsweise von CA ARCserve Central Virtual Standby (siehe Seite 12)
CA ARCserve Central Applications-Bookshelf (siehe Seite 14)

Einführung

CA ARCserve Central Applications verbindet wichtige Datenschutz- und -Managementtechnologien mit einem Ökosystem von Zielanwendungen, die im Einklang miteinander funktionieren, um sowohl Innen- und Außenschutz als auch das Kopieren, Verschieben und Transformieren von Daten quer durch globale Umgebungen zu ermöglichen.

CA ARCserve Central Applications sind einfach zu verwenden, handzuhaben und zu installieren. Sie bieten Organisationen eine automatische Kontrolle über ihre Informationen, um fundierte Entscheidungen über den Zugriff, die Verfügbarkeit und Sicherheit ihrer Daten auf der Basis des allgemeinen Geschäftswerts zu treffen.

CA ARCserve Central Applications umfasst neben anderen Anwendungen CA ARCserve Central Virtual Standby. CA ARCserve Central Virtual Standby lässt sich mit CA ARCserve D2D integrieren und ermöglicht es Ihnen, virtuelle Rechner von CA ARCserve D2D-Sicherungssitzungen aus bereitzustellen. Die Anwendung bietet Ihnen folgende Möglichkeiten:

- Konvertieren Sie CA ARCserve D2D-Wiederherstellungspunkte, die auf den CA ARCserve D2D-Zielgeräten gespeichert sind, auf der Basis eines Ablaufplans in VMware-Dateien für virtuelle VMware-Partitionen (VMDK) oder Microsoft-Virtual-PC-Dateien für virtuelle Partitionen (VHD). Von den Wiederherstellungspunkt-Snapshots aus können Sie virtuelle Rechner dazu befähigen, als CA ARCserve D2D-Quellserver zu arbeiten, falls Ihre Quellserver fehlschlagen.
- Konvertierungsrichtlinien auf CA ARCserve D2D-Quellserver übertragen.
- Sie können Wiederherstellungspunkt-Snapshots auf virtuellen Rechnern speichern, die auf VMware ESX Server oder Windows Hyper-V basieren.
- Sie können virtuelle Rechner manuell oder automatisch starten, wenn eine Notfallsituation auftritt.
- Sie können Daten von Wiederherstellungspunkt-Snapshots zu ursprünglichen oder alternativen Quellservern (V2P-Wiederherstellungen) wiederherstellen.

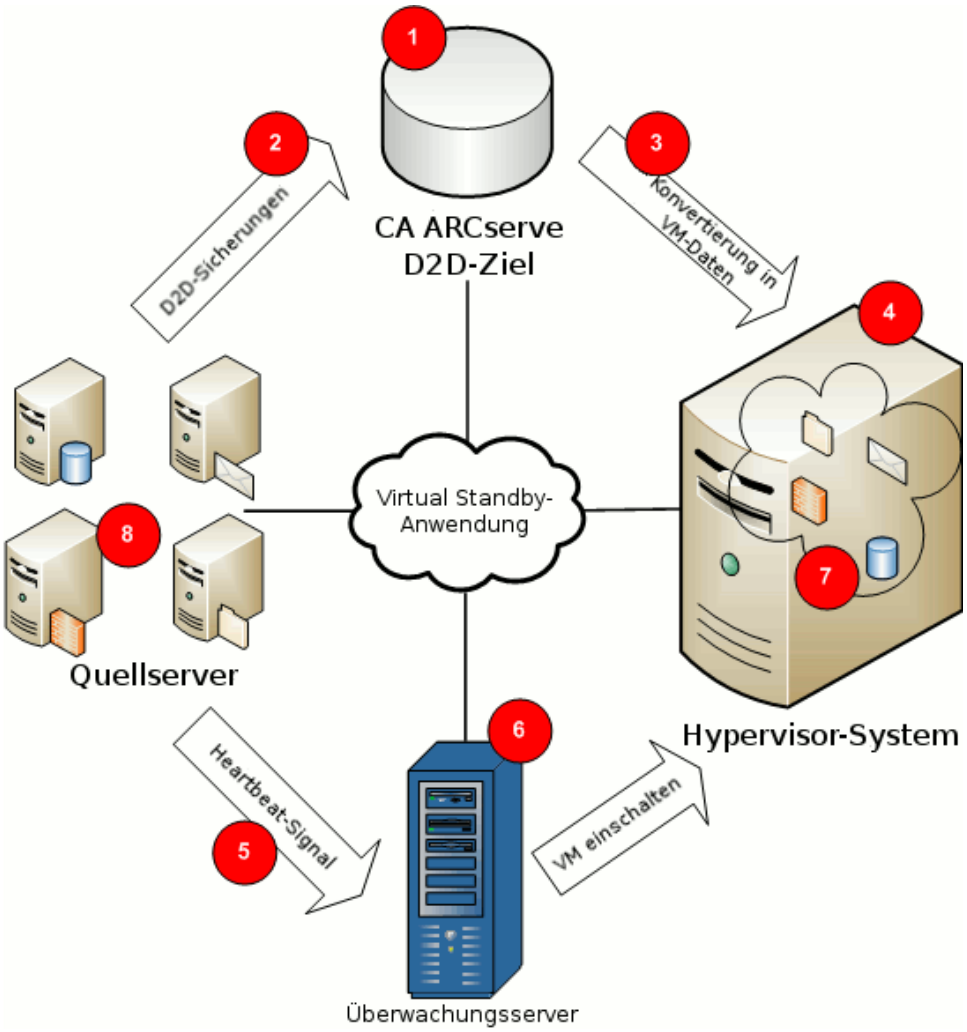
Funktionsweise von CA ARCserve Central Virtual Standby

Mit Virtual Standby können Sie die CA ARCserve D2D-Quellserver, die in Ihrer Umgebung arbeiten, wie folgt schützen:

- Konvertieren Sie CA ARCserve D2D-Wiederherstellungspunkte, die auf den CA ARCserve D2D-Zielgeräten gespeichert sind, auf der Basis eines Ablaufplans in VMware-Dateien für virtuelle VMware-Partitionen (VMDK) oder Microsoft-Virtual-PC-Dateien für virtuelle Partitionen (VHD).
- Kopieren Sie die konvertierten Daten auf ein Hypervisor-System.
- Erstellen Sie Wiederherstellungspunkt-Snapshots anhand der VMDK- oder VHD-Daten.
- Überwachen Sie den Zustand des Quellservers.
- Nehmen Sie, wenn Sie eine Notsituation festgestellt haben, virtuelle Rechner automatisch von den Wiederherstellungspunkt-Snapshots in Betrieb.

  Hinweis: Virtual Standby kann so konfiguriert werden, dass es Wiederherstellungspunkt-Snapshots automatisch oder manuell in Betrieb nimmt, wenn ein Problem auftritt.
- Stellen Sie die Daten vom virtuellen Rechner auf dem Quellserver wieder her, nachdem Sie die Probleme auf dem Quellserver behoben haben.

Die folgende Abbildung veranschaulicht diesen Prozess.



CA ARCserve D2D (1) erstellt Wiederherstellungspunkte auf dem CA ARCserve D2D-Zielgerät (2) für die Quellserver. Virtual Standby konvertiert die Wiederherstellungspunkte in das Format für virtuelle Rechner (3) und speichert die Daten als Wiederherstellungspunkt-Snapshots auf dem Hypervisor-System (4).

Der Überwachungsserver (6) überwacht den Zustand der Quellserver. Wenn der Überwachungsserver kein Heartbeat-Signal (5) von Quellserver (8) entdecken kann, schaltet der Überwachungsserver einen reduziert bereitgestellten virtuellen Rechner (7) auf dem Hypervisor-System (4) ein, um als Quellserver zu fungieren, indem im aktuellsten Wiederherstellungspunkt-Snapshot enthaltene Daten verwendet werden. CA ARCserve Central Virtual Standby erstellt eine virtuelle Rechnerpartition, deren Größe dem Quellserver entspricht.

Nachdem Sie die Probleme auf dem Quellserver behoben haben, können Sie den Quellserver (8) mithilfe der Daten (7), die in der VM gespeichert sind, auf dem Hypervisor-System wieder in seinen aktuellen Status bringen.

Hinweis: Wenn Sie den virtuellen Rechner sichern möchten, nachdem er eingeschaltet wurde, können Sie eine CA ARCserve D2D-Sicherungsrichtlinie auf dem virtuellen Rechner mithilfe von CA ARCserve Central Protection Manager bereitstellen.

CA ARCserve Central Applications-Bookshelf

Die Inhalte dieser CA ARCserve Central Applications-Hilfe sind auch als Benutzerhandbuch im PDF-Format verfügbar. Auf die neueste PDF-Version dieses Handbuchs und der Hilfe kann vom CA ARCserve Central Applications-Bookshelf aus zugegriffen werden.

Die Dateien mit CA ARCserve Central Applications-Versionshinweisen enthalten Informationen bezüglich Systemanforderungen, unterstützte Betriebssysteme, Support bei der Wiederherstellung der Anwendung und andere Informationen, die Sie kennen sollten, bevor Sie dieses Produkt installieren. Außerdem enthalten die Versionshinweise eine Liste bekannter Probleme, derer Sie sich bewusst sein sollten, bevor Sie CA ARCserve Central Applications verwenden. Auf die aktuelle Version der Versionshinweise kann vom CA ARCserve Central Applications-Bookshelf aus zugegriffen werden.

Kapitel 2: Installation von CA ARCserve Central Virtual Standby

Dieses Kapitel enthält folgende Themen:

Erforderliche Installationsaufgaben (siehe Seite 15)
Installationshinweise (siehe Seite 17)
Installation von CA ARCserve Central Virtual Standby (siehe Seite 18)
Deinstallieren von CA ARCserve Central Virtual Standby (siehe Seite 20)
CA ARCserve Central Virtual Standby automatisch installieren (siehe Seite 20)
CA ARCserve Central Virtual Standby automatisch deinstallieren (siehe Seite 23)

Erforderliche Installationsaufgaben

Führen Sie vor der Installation von CA ARCserve Central Virtual Standby die folgenden vorbereitenden Aufgaben durch:

- Stellen Sie sicher, dass die aktuellste unterstützte Version von CA ARCserve D2D auf folgenden Elementen installiert ist:
  - Der Quellserver, die Sie schützen wollen
  - Der Server, den Sie festgelegt haben, um Snapshots für Wiederherstellungspunkte zu speichern

    Hinweis: Diese Anforderung gilt nur für Hyper-V-Server, die dafür konfiguriert sind, den Zustand von Knoten zu überwachen (physische oder virtuelle Rechner), und die Wiederherstellungspunkt-Snapshots für die Knoten zu speichern.
  - Der Server, den Sie festgelegt haben, um die Quellserver zu überwachen

  Hinweis: Wenn Sie CA ARCserve Central Protection Manager in Ihrer Produktionsumgebung installiert haben, können Sie CA ARCserve D2D mithilfe der D2D-Bereitstellung auf mehreren Remote-Knoten installieren. Weitere Informationen finden Sie im CA ARCserve Central Protection Manager-Benutzerhandbuch.
- Stellen Sie in Hyper-V-Umgebungen sicher, dass CA ARCserve D2D im Hyper-V-Hostsystem installiert ist. In Hyper-V-Umgebungen fungieren Hyper-V-Hostsysteme als Speicherort für Wiederherstellungspunkt-Snapshots und als Überwachungsserver.

- Stellen Sie in VMware-Umgebungen sicher, dass CA ARCserve D2D im Proxy-System installiert ist.

  Hinweis: In VMware-Umgebungen fungiert der Zieldatenspeicher des ESX Servers als Speicherort für Wiederherstellungspunkt-Snapshots. Das Proxysystem kann optional als Überwachungsserver fungieren.

- Überprüfen Sie die Datei mit den Versionshinweisen. Die Datei mit den Versionshinweisen enthält eine Beschreibung der Systemanforderungen, unterstützten Betriebssystemen und eine Liste der Probleme, die in dieser Version bekannt sind.
- Stellen Sie sicher, dass Ihr System die Mindestanforderungen für die Hardware und Software erfüllt, die für die Installation von CA ARCserve Central Virtual Standby erforderlich sind.
- Stellen Sie sicher, dass Sie über Administratorrechte oder die entsprechende Berechtigung zum Installieren von Software auf den Computern verfügen, auf denen Sie CA ARCserve Central Virtual Standby installieren möchten.
- Stellen Sie sicher, dass Ihr Konto über VMware vCenter- oder ESX Server-Administratorberechtigungen und Windows-Administratorberechtigungen verfügt. Die Rolle "Global License" ist im Konto auf dem vCenter Server-System oder ESX Server-System notwendig, damit VDDK-Vorgänge erfolgreich durchgeführt werden können.
- Prüfen Sie, ob Sie die Benutzernamen und Kennwörter der Computer haben, auf denen Sie CA ARCserve Central Virtual Standby, das Sie besitzen, installieren.
- Stellen Sie sicher, dass Sie die Hostnamen oder IP-Adressen der Computer haben, die Ihre Quellrechner überwachen sollen.
- Stellen Sie sicher, dass Sie die Hostnamen oder IP-Adresse der Computer haben, auf denen Ihre Snapshots der Wiederherstellungspunkte gespeichert werden sollen.
- Prüfen Sie, ob Sie alle Lizenzen haben, die benötigt werden, um das Ihnen verfügbare CA ARCserve Central Virtual Standby zu installieren.
- Überprüfen Sie, ob die CA ARCserve D2D-Versionsnummer und die CA ARCserve Central Virtual Standby-Versionsnummer übereinstimmen.

Installationshinweise

Bevor Sie CA ARCserve Central Virtual Standby installieren, beachten Sie folgende Installationshinweise:

- Das CA ARCserve Central Applications-Installationspaket installiert ein Modul namens CA ARCserve Central Applications Server. CA ARCserve Central Applications Server ist ein Modul, das allen CA ARCserve Central Applications bekannt ist. Das Modul enthält den Webservice, Binärdateien und Konfigurationen, die CA ARCserve Central Applications miteinander kommunizieren lassen.

  Wenn Sie CA ARCserve Central Applications installieren, installiert das Installationspaket das CA ARCserve Central Applications Server-Modul, bevor es die Produktkomponenten installiert. Wenn es notwendig wird, einen Patch für CA ARCserve Central Applications anzuwenden, aktualisiert der Patch das Modul, bevor er die Produktkomponenten aktualisiert.

- CA ARCserve D2D installiert VMware Virtual Disk Development Kit (VDDK) auf allen Rechnern, auf denen Sie CA ARCserve D2D installieren. Sie müssen VDDK nicht herunterladen und auf Ihren Virtual Standby-Proxy-Systemen installieren.

  Wenn Sie eine neuere VDDK-Version verwenden wollen, laden Sie VDDK herunter und installieren Sie es, und ersetzen Sie dann den Wert des unter HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D angegebenen VDDKDirectory-Registrierungseintrags durch den des Installationsordners, in dem das neue VDDK installiert wurde.

  Der Standardspeicherort für VDDK lautet folgendermaßen:

  - **x64-Betriebssystem:**

    ```
    C:\Programme (x86)\VMware\VMware Virtual Disk Development Kit
    ```

    Hinweis: Entzippen Sie die VDDK64.zip-Datei vom VDDK-Installationsverzeichnis in den VDDK64-Ordner.

    Zum Beispiel: C:\Programme (x86)\VMware\VMware Virtual Disk Development Kit\VDDK64

  - **x86-Betriebssystem:**

    ```
    C:\Programme\VMware\VMware Virtual Disk Development Kit
    ```

- Hinweis: CA ARCserve Central Virtual Standby unterstützt keine Erstellung virtueller Datenträger-Images auf komprimierten Volumes oder Volumes, die vom Dateisystem verschlüsselt werden.

  Hinweis: Diese Beschränkung bezieht sich nur auf Hypervisoren von Hyper-V.

- CA ARCserve Central Virtual Standby unterstützt keinen Schutz von virtuellen VMware-Rechnern, die mithilfe von JIS2004-Unicode-Zeichen benannt wurden.

- CA ARCserve Central Virtual Standby unterstützt nicht den Schutz von virtuellen Rechnern, die eine Datenträgergröße von 2 Terabyte überschreiten.

Installation von CA ARCserve Central Virtual Standby

Der Installationsassistent hilft Ihnen dabei, führt Sie durch den Prozess, CA ARCserve Central Applications einmal oder mehrmals zu installieren.

Hinweis: Bevor Sie die Anwendung installieren, überprüfen Sie die Datei mit den Versionshinweisen und stellen Sie sicher, dass alle in Vorbereitende Aufgaben beschriebene Aufgaben ausgeführt sind.

So installieren Sie CA ARCserve Central Virtual Standby

1. Laden Sie das CA ARCserve Central Applications-Installationspaket auf den Computer herunter, auf dem Sie die Anwendung installieren möchten, und doppelklicken Sie dann auf die Setup-Datei.

   Das Installationspaket extrahiert seine Inhalte auf Ihren Computer und daraufhin öffnet sich das Dialogfeld "Erforderliche Komponenten".

2. Klicken Sie im Dialogfeld "Erforderliche Komponenten" auf "Installieren".

   Hinweis: Das Dialogfeld "Erforderliche Komponenten" wird nur angezeigt, wenn Setup die erforderlichen Komponenten nicht auf dem Zielcomputer installiert findet.

   Nachdem Setup die erforderlichen Komponenten installiert hat, öffnet sich das Dialogfeld "Lizenzvereinbarung".

3. Füllen Sie die erforderlichen Optionen auf der Lizenzvereinbarung aus, und klicken Sie auf "Weiter".

   Das Dialogfeld "Konfiguration" wird geöffnet.

4. Führen Sie auf dem Dialogfeld "Konfiguration" folgende Schritte aus:

   - **Komponenten**: Geben Sie die Anwendungen an, die Sie installieren wollen.

     Hinweis: Wenn Sie diese Anwendung mithilfe des Suite-Installationspakets installieren, können Sie mehrere Anwendungen installieren.

   - **Speicherort**: Akzeptieren Sie den Standardspeicherort für die Installation oder klicken Sie auf "Durchsuchen", um einen alternativen Installationsspeicherort anzugeben. Der Standardspeicherort lautet folgendermaßen:

     ```
     C:\Programme\CA\ARCserve Central Applications
     ```

   - **Festplatteninformationen**: Stellen Sie sicher, dass Ihre Festplatte über ausreichenden Speicherplatz verfügt, um die Anwendungen zu installieren.

   - **Name des Windows-Administrators**: Geben Sie den Benutzernamen des Windows-Administratorkontos unter Verwendung der folgenden Syntax an:

     ```
     Domäne\Benutzername
     ```

- **Kennwort:** Geben Sie das Kennwort für das Benutzerkonto an.
- **Portnummer angeben:** Geben Sie die Portnummer an, die Sie verwenden wollen, um mit der webbasierten Benutzeroberfläche zu kommunizieren. Als Best Practice sollten Sie die standardmäßige Portnummer akzeptieren. Die standardmäßige Portnummer lautet:

  `8015`

  Hinweis: Wenn Sie eine alternative Portnummer angeben wollen, liegen die verfügbaren Portnummern zwischen 1024 und 65535. Bevor Sie eine alternative Portnummer angeben, überprüfen Sie, ob die festgelegte Portnummer frei und zur Verwendung verfügbar ist. Setup hindert Sie daran, die Anwendung mithilfe eines Ports zu installieren, der nicht zur Verwendung verfügbar ist.

- **Für Web-Kommunikationen HTTPS verwenden:** Legen Sie die Verwendung der HTTPS-Kommunikation für Datenübertragung fest. Standardmäßig ist diese Option deaktiviert.

  Hinweis: Sichere HTTPS-Kommunikation bietet eine höhere Sicherheitsebene als HTTP-Kommunikation. HTTPS ist das empfohlene Kommunikationsprotokoll, wenn Sie in Ihrem Netzwerk vertrauliche Informationen übertragen.

- **Lassen Sie zu, dass Setup die Dienste und Programme von CA ARCserve Central Applications als Ausnahmen für die Windows Firewall registriert --**Stellen Sie sicher, dass das Kontrollkästchen neben dieser Option aktiviert ist. Firewall-Ausnahmen sind erforderlich, wenn Sie CA ARCserve Central Applications von Remote-Rechnern aus konfigurieren und verwalten möchten.

  Hinweis: Benutzer, die die Anwendung lokal verwenden, brauchen keine Firewall-Ausnahmen zu registrieren.

Klicken Sie auf "Weiter".

Der Installationsprozess wird ausgeführt.

Nachdem der Installationsprozess abgeschlossen ist, öffnet sich das Dialogfeld "Installationsbericht".

5. Das Dialogfeld "Installationsbericht" fasst die Installation zusammen. Wenn Sie jetzt nach Aktualisierungen für die Anwendung suchen wollen, klicken Sie auf "Nach Aktualisierungen suchen" und danach auf "Fertig stellen".

Die Anwendung wird installiert.

Deinstallieren von CA ARCserve Central Virtual Standby

Sie können die Anwendung mithilfe von Programmen und in der Windows Systemsteuerung befindlichen Funktionen deinstallieren.

Gehen Sie wie folgt vor:

1. Klicken Sie im Windows Startmenü auf "Start" und klicken Sie auf "Systemsteuerung".

   Die Windows Systemsteuerung wird geöffnet.

2. Klicken Sie in der Windows Systemsteuerung auf die Dropdown-Liste neben "Anzeigen" und klicken Sie danach auf "Große Symbole" oder "Kleine Symbole".

   Die Symbole für die Anwendungen der Windows Systemsteuerung werden in einer Rasteransicht angezeigt.

3. Klicken Sie auf Programme und Funktionen.

   Das Fenster "Programm deinstallieren oder ändern" öffnet sich.

4. Suchen Sie die Anwendung, die Sie deinstallieren wollen, und klicken Sie darauf.

   Klicken Sie mit der rechten Maustaste auf die Anwendung und im Pop-up-Menü auf "Deinstallieren".

   Folgen Sie den Bildschirmanweisungen, um die Anwendung zu deinstallieren.

Die Anwendung wird deinstalliert.

CA ARCserve Central Virtual Standby automatisch installieren

Mit CA ARCserve Central Applications können Sie CA ARCserve Central Virtual Standby automatisch installieren. Bei der automatischen Installation ist kein Benutzereingriff erforderlich. Die folgenden Schritte beschreiben, wie sie die Anwendung mithilfe der Windows-Befehlszeile installieren können.

So installieren Sie CA ARCserve Central Virtual Standby automatisch

1. Öffnen Sie die Windows-Befehlszeile auf dem Computer, auf dem Sie den automatischen Installationsvorgang starten wollen.

2. Laden Sie das selbstextrahierende
   CA ARCserve Central Applications-Installationspaket auf Ihren Computer herunter.

   Starten Sie den automatischen Installationsvorgang mithilfe der folgenden Befehlszeilen-Syntax:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q
   -Path:<INSTALLATIONSVERZEICHNIS> -Port:<PORT> -U:<Benutzername> -P:<Kennwort>
   -Products:<Produktliste>"
   ```

Verwendung:

s

Lässt Sie das ausführbare Dateipaket im automatischen Modus ausführen.

v

Lässt Sie zusätzliche Befehlszeilenoptionen angeben.

q

Lässt Sie die Anwendung im automatischen Modus installieren.

-Path:<INSTALLATIONSVERZEICHNIS>

(Optional) Lässt Sie den Zielinstallationspfad festlegen.

Beispiel:

```
-Path:“C:\Programme\CA\ARCserve Central Applications”
```

Hinweis: Wenn der Wert für INSTALLATIONSVERZEICHNIS ein Leerzeichen enthält, setzen Sie den Pfad zwischen umgekehrte Schrägstriche und Anführungszeichen. Zudem kann der Pfad nicht mit einem umgekehrten Schrägstrich enden.

-Port:<PORT>

(Optional) Lässt Sie die Portnummer für die Kommunikation festlegen.

Beispiel:

```
-Port:8015
```

-U:<Benutzername>

Lässt Sie den Benutzernamen festlegen, der verwendet werden soll, um die Anwendung zu installieren und auszuführen.

Hinweis: Der Benutzername muss ein Administratorkonto oder ein Konto mit Administratorrechten sein.

-P:<Kennwort>

Lässt Sie das Kennwort für den Benutzernamen festlegen.

-Products:<ProductList>

(Optional) Ermöglicht es Ihnen, die CA ARCserve Central Applications-Anwendungen anzugeben, die automatisch installiert werden sollen. Wenn Sie keinen Wert für dieses Argument angeben, installiert der automatische Installationsvorgang alle Komponenten der CA ARCserve Central Applications-Anwendungen.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Alle CA ARCserve Central Applications

ALLE

Hinweis: Die folgenden Beispiele beschreiben die Syntax, die erforderlich ist, um eine, zwei, drei oder alle CA ARCserve Central Applications automatisch zu installieren:

```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

Die Anwendung wird automatisch installiert.

CA ARCserve Central Virtual Standby automatisch deinstallieren

Mit CA ARCserve Central Applications können Sie CA ARCserve Central Virtual Standby automatisch deinstallieren. Bei der automatischen Installation ist kein Benutzereingriff erforderlich. Die folgenden Schritte beschreiben, wie sie die Anwendung mithilfe der Windows-Befehlszeile deinstallieren können.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, von dem Sie die Anwendung deinstallieren möchten.

   Hinweis: Sie müssen sich über ein administratives Konto oder ein Konto mit administrativen Berechtigungen anmelden.

2. Öffnen Sie die Windows-Befehlszeile, und führen Sie folgenden Befehl aus, um den automatischen Deinstallationsvorgang zu starten:

   ```
   <INSTALLATIONSVERZEICHNIS>%\Setup\uninstall.exe /q /p <Produktcode>
   ```

   Oder

   ```
   <INSTALLATIONSVERZEICHNIS>%\Setup\uninstall.exe /q /ALL
   ```

   Beispiel: Mit der folgende Syntax können Sie CA ARCserve Central Virtual Standby automatisch deinstallieren.

   ```
   "%Programme%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED4835-964B-484B-A395-E2DF12E6F73D}
   ```

Verwendung:

<INSTALLATIONSVERZEICHNIS>

Hier können Sie das Verzeichnis angeben, in dem die Anwendung installiert ist.

Hinweis: Führen Sie die Syntax aus, die der Architektur des Betriebssystems des Computers entspricht.

<Produktcode>

Hier können Sie die Anwendung angeben, die automatisch deinstalliert werden soll.

Hinweis: Der automatische Deinstallationsvorgang lässt Sie eine oder mehrere CA ARCserve Central Applications deinstallieren. Verwenden Sie die folgenden Produktcodes, um CA ARCserve Central Applications automatisch zu deinstallieren.

CA ARCserve Central Host-Based VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

CA ARCserve Central Protection Manager

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

Die Anwendung wird automatisch deinstalliert.

Kapitel 3: Erste Schritte mit CA ARCserve Central Virtual Standby

Folgende Abschnitte beschreiben, wie CA ARCserve Central Virtual Standby konfiguriert werde sollte, um CA ARCserve D2D-Knoten zu schützen.

Hinweis: Um die in diesem Abschnitt beschriebenen Konfigurationen durchführen zu können, stellen Sie sicher, dass alle erforderlichen Installationsaufgaben (siehe Seite 15) abgeschlossen sind.

Dieses Kapitel enthält folgende Themen:

Stellen Sie sicher, dass der CA ARCserve Central Virtual Standby-Server mit den Knoten kommunizieren kann. (siehe Seite 26)
Anmeldung bei CA ARCserve Central Virtual Standby (siehe Seite 27)
Hinzufügen von Knoten nach IP-Adresse oder Knotennamen (siehe Seite 28)
Hinzufügen von Knotengruppen (siehe Seite 29)
Geben Sie das ESX Server- oder vCenter Server-System für VMware-basierte Knoten an (siehe Seite 30)
Erstellen von Richtlinien (siehe Seite 32)
Zuweisen von Knoten zu Richtlinien (siehe Seite 39)
Bereitstellen von Richtlinien (siehe Seite 40)

Stellen Sie sicher, dass der CA ARCserve Central Virtual Standby-Server mit den Knoten kommunizieren kann.

Hinweis: Dies ist ein optionaler Schritt, um CA ARCserve Central Virtual Standby so zu konfigurieren, dass Knoten geschützt werden.

Um dabei zu helfen, sicherzustellen, dass CA ARCserve Central Virtual Standby Richtlinien für Knoten bereitstellen und Knoten schützen kann, stellen Sie sicher, dass der Virtual Standby-Server und die Knoten, die Sie schützen möchten, unter Verwendung ihrer Hostnamen kommunizieren können.

So stellen Sie sicher, dass der CA ARCserve Central Virtual Standby-Server mit den Knoten kommunizieren kann

1. Pingen Sie vom CA ARCserve Central Virtual Standby-Server aus die Knoten, die Sie unter Verwendung der Hostnamen der Knoten schützen möchten.
2. Pingen Sie von den Knoten aus, die Sie schützen wollen, den CA ARCserve Central Virtual Standby-Server mit dem Hostnamen des Servers an.

Anmeldung bei CA ARCserve Central Virtual Standby

Sie können sich bei CA ARCserve Central Virtual Standby direkt über den Rechner anmelden, auf dem die Anwendung installiert ist, oder Sie können sich mithilfe eines unterstützten Browsers über einen Remote-Rechner anmelden. Eine vollständige Liste der unterstützten Browser finden Sie in den *CA ARCserve Central Virtual Standby-Versionshinweisen*.

So melden Sie sich bei CA ARCserve Central Virtual Standby an:

1. Führen Sie eine der folgenden Optionen aus:

   - Wenn Sie bei einem Server angemeldet sind, auf dem CA ARCserve Central Virtual Standby installiert ist, starten Sie die Anwendung von Ihren Programmdateien aus.

     Ein Browserfenster mit dem CA ARCserve Central Virtual Standby-Anmeldebildschirm wird angezeigt.

     Vervollständigen Sie im Anmeldebildschirm folgende Felder:

     - Benutzername
     - Kennwort

     Klicken Sie auf "Anmelden".

   - Wenn Sie nicht bei dem Server, auf dem CA ARCserve Central Virtual Standby installiert ist, angemeldet sind, öffnen Sie ein Browserfenster und geben Sie in der Adressleiste folgende URL ein:

     ```
     http://<CA ARCserve Central Application Server Name>:<Portnummer>/virtualstandby/
     ```

     Hinweis: Wenn CA ARCserve Central Virtual Standby installiert ist, können Sie den Hostnamen oder die IP-Adresse des Servers angeben. Die standardmäßige Port-Nummer lautet 8015.

     Drücken Sie die Eingabetaste.

     Ein Browserfenster mit dem CA ARCserve Central Virtual Standby-Anmeldebildschirm wird angezeigt.

     Vervollständigen Sie im Anmeldebildschirm folgende Felder:

     - Benutzername
     - Kennwort

     Klicken Sie auf "Anmelden".

   Sie werden bei CA ARCserve Central Virtual Standby angemeldet, und die Startseite wird geöffnet.

Hinzufügen von Knoten nach IP-Adresse oder Knotennamen

Virtual Standby lässt Sie Knoten hinzufügen, die auf der IP-Adresse oder dem Knotennamen basieren. Fügen Sie die CA ARCserve D2D-Quellknoten hinzu, die Sie schützen möchten.

So fügen Sie Knoten nach IP-Adresse oder Knotennamen hinzu

1. Klicken Sie auf der Startseite in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt:

2. Klicken Sie in der Symbolleiste "Knoten" auf "Hinzufügen", und dann im Pop-up-Menü auf "Knoten nach IP/Namen hinzufügen".

   Das Dialogfeld "Knoten nach IP/Namen hinzufügen" wird geöffnet.

3. Füllen Sie folgende Felder im Dialogfeld "Knoten nach IP/Namen hinzufügen" aus:

   - **IP/Knotenname:** Lässt Sie die IP-Adresse oder den Namen des Knotens festlegen.
   - **Beschreibung:** Lässt Sie eine Beschreibung für den Knoten festlegen.
   - **Benutzername:** Lässt Sie den Benutzernamen festlegen, der für die Anmeldung am Knoten erforderlich ist.
   - **Kennwort:** Lässt Sie das Kennwort festlegen, das für die Anmeldung am Knoten erforderlich ist.

   Klicken Sie auf "OK".

4. (Optional) Wenn der neu hinzugefügte Knoten nicht in der Knotenliste angezeigt wird, klicken Sie in der Symbolleiste "Knoten" auf "Aktualisieren".

Das Dialogfeld "Knoten nach IP/Namen hinzufügen" schließt sich und der Knoten ist hinzugefügt.

Hinzufügen von Knotengruppen

Knotengruppen lassen Sie eine Sammlung von auf eine Gemeinsamkeit basierenden CA ARCserve D2D-Quellcomputern verwalten. Zum Beispiel können Sie Knotengruppen definieren, die nach der Abteilung klassifiziert sind, die sie unterstützen: Buchhaltung, Marketing, Recht, Personal, und so weiter.

Die Anwendung enthält die folgenden Knotengruppen:

- **Standardgruppen:**
  - **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
  - **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
  - **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
  - **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft SQL Server ist auf dem Knoten installiert.
  - **Exchange:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft Exchange Server ist auf dem Knoten installiert.

  Hinweis: Sie können die Standardknotengruppen nicht ändern oder löschen.
- **Benutzerdefinierte Gruppen:** Enthält benutzerdefinierte Knotengruppen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.
2. Klicken Sie in der Symbolleiste "Knotengruppe" auf "Hinzufügen".

   Das Dialogfeld "Gruppe hinzufügen" öffnet sich und die Knoten werden in der Liste der verfügbaren Knoten angezeigt.
3. Geben Sie einen Gruppennamen für die Knotengruppe an.
4. Geben Sie im Dialogfeld "Gruppe hinzufügen" folgende Felder an:
   - **Gruppe:** Wählen Sie den Gruppennamen aus, der die Knoten enthält, die Sie zuweisen möchten.
   - **Knotennamenfilter:** Lässt Sie die verfügbaren Knoten basierend auf einer Gemeinsamkeit filtern.

     Hinweis: Das Feld "Knotenname" unterstützt die Verwendung von Platzhalterzeichen.

     Acc* lässt Sie beispielsweise alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt. Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

5. Um Knoten zur Knotengruppe hinzuzufügen, wählen Sie die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf den einzelnen Rechtspfeil.

   Die Knoten verschieben sich von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" und werden der Knotengruppe zugewiesen.

   Hinweis: Um alle Knoten auszuwählen und aus der aktuellen Gruppe zu verschieben, klicken Sie auf den doppelten Rechtspfeil.

6. (Optional) Um Knoten von der Liste "Ausgewählte Knoten" in die Liste "Verfügbare Knoten" zu verschieben, klicken Sie auf den einzelnen Linkspfeil.

   Hinweis: Um alle Knoten auszuwählen und in der aktuellen Gruppe zu verschieben, klicken Sie auf den doppelten Linkspfeil.

7. Klicken Sie auf "OK".

Die Knotengruppe wird hinzugefügt.

Geben Sie das ESX Server- oder vCenter Server-System für VMware-basierte Knoten an

Hinweis: Der folgende Vorgang bezieht sich auf nur VMware-basierte Quellknoten virtueller Rechner.

Möglicherweise kann Virtual Standby in bestimmten VMware-basierten Implementierungen keine Quellknoten entdecken, die als virtuelle Rechner auf ESX Server- und vCenter Server-Systemen konfiguriert sind. Durch dieses Verhalten kann Virtual Standby für die Knoten nicht die richtige Lizenz anwenden, Richtlinien bereitstellen und Konvertierungsjobs ausführen.

Der folgende Vorgang ermöglicht es Ihnen, den Hostnamen oder die IP-Adresse des ESX Server- oder vCenter Server-Systems anzugeben, auf dem sich die Knoten befinden. Nachdem Sie den Vorgang abgeschlossen haben, kann Virtual Standby Lizenzen entdecken und anwenden, Richtlinien bereitstellen und Konvertierungsjobs für Knoten ausführen, die Sie schützen möchten. Wenn sich auf einem ESX Server- oder vCenter Server-System mehrere virtuelle Rechner befinden, die als Quellknoten fungieren, können Sie im beschriebenen Vorgang für alle Knoten dieselbe Lizenz verwenden. Dies hilft Ihnen dabei, die Gesamtkosten für den Schutz der Quellknoten zu senken.

So geben Sie das ESX Server- oder vCenter Server-System für VMware-basierte Knoten an

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Menüleiste "Gruppen" auf die Gruppe "Alle Knoten" oder klicken Sie auf den Gruppennamen, der den Knoten enthält, den Sie aktualisieren wollen.

   Die der Gruppe zugeordneten Knoten werden in der Knotenliste angezeigt.

3. Klicken Sie auf den Knoten, den Sie aktualisieren möchten, und klicken Sie anschließend im Pop-up-Menü auf "ESX Server angeben".

   Das Dialogfeld "ESX Server angeben" wird geöffnet.

   Hinweis: Wenn die Anwendung entdeckt, dass VMware Tools nicht auf dem vom ESX Server- oder vCenter Server-System verwalteten virtuellen Rechner installiert ist, sich der virtuelle Rechner auf einem Hyper-V-System befindet, oder der entdeckte Knoten kein virtueller Rechner ist, wird eine Fehlermeldung angezeigt.

4. Füllen Sie im Dialogfeld "ESX Server angeben" folgende Felder aus:

   - ESX/vCenter-Host

     Hinweis: Geben Sie den Hostnamen oder die IP-Adresse des ESX Server- oder vCenter Server-Systems an.

   - Benutzername
   - Kennwort
   - Port

     Hinweis: Der Standardkommunikationsport ist 443. Wenn der Knoten mit dem ESX Server- oder vCenter Server-System über eine andere Portnummer kommuniziert, geben Sie die Portnummer an, die verwendet wird.

   - Protokoll

     Hinweis: Das Standardkommunikationsprotokoll ist HTTPS. Wenn der Knoten mit dem ESX Server- oder vCenter Server-System über HTTP kommuniziert, klicken Sie auf "HTTP".

   Klicken Sie auf "OK".

Das ESX Server- oder vCenter Server-System wird dem Knoten zugewiesen.

Erstellen von Richtlinien

Mit Virtual Standby können Sie benutzerdefinierte Konvertierungsrichtlinien angeben, die Sie CA ARCserve D2D-Knoten zuweisen.

Hinweis: Um Richtlinien zu erstellen, muss CA ARCserve D2D auf dem Überwachungsserver installiert sein.

So erstellen Sie Richtlinien

1. Melden Sie sich beim Virtual Standby-Server an und öffnen Sie Virtual Standby.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Richtlinien".

   Das Fenster "Richtlinien" wird geöffnet.

2. Klicken Sie in der Symbolleiste "Richtlinien" auf "Neu".

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Geben Sie im Feld "Richtlinienname" einen Namen für die Richtlinie ein.

   Klicken Sie auf die Registerkarte "Virtual Standby".

   Die Optionen "Virtualisierungsserver", "Virtueller Rechner" und "Aushilfseinstellungen" werden angezeigt.

4. Klicken Sie auf "Virtualisierungsserver".

   Die Optionen für "Virtualisierungsserver" werden angezeigt.

5. Vervollständigen Sie die folgenden Optionen für "Virtualisierungsserver":

   VMware-Systeme:

   - **Virtualisierungstyp:** Klicken Sie auf "VMware".
   - **ESX-Host/-Virtual Center**: Legen Sie den Hostnamen des ESX- oder vCenter Server-Systems fest.
   - **Benutzername:** Legen Sie den Benutzernamen fest, der für die Anmeldung beim VMware-System erforderlich ist.

     Hinweis: Das Konto, das Sie angeben, muss ein administratives Konto oder ein Konto mit administrativen Berechtigungen für das ESX- oder vCenter Server-System sein.
   - **Kennwort:** Legen Sie das Kennwort für den Benutzernamen fest, für den die Anmeldung beim VMware-System erfolgen soll.
   - **Protokoll:** Legen Sie HTTP oder HTTPS als Protokoll an, das Sie für die Kommunikation zwischen dem CA ARCserve D2D-Quellknoten und dem Überwachungsserver verwenden möchten.

- **Port:** Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Überwachungsserver verwenden wollen.
- **ESX-Knoten:** Die Werte in diesem Feld variieren basierend auf dem Wert, der im Feld "ESX-Host/vCenter" angegeben wird:
  - **ESX Server-Systeme:** Wenn Sie ein ESX Server-System im Feld "ESX-Host/vCenter" angeben, zeigt dieses Feld den Hostnamen des ESX Server-Systems an.
  - **vCenter Server-Systeme:** Wenn Sie ein vCenter Server-System im Feld "ESX-Host/vCenter" angeben, können Sie in diesem Feld (aus einer Drop-down-Liste) das ESX Server-System angeben, das Sie mit dieser Richtlinie verknüpfen möchten.
- **Überwachungsserver:** Legen Sie den Hostnamen des Servers fest, bei dem Sie den Status des Quellservers überwachen wollen.

  Hinweis: Der Überwachungsserver kann ein beliebiger physischer Computer oder virtueller Rechner sein, vorausgesetzt, dass er kein Proxy-Server für eine CA ARCserve Central Host-Based VM Backup-Implementierung ist.
- **Benutzername:** Legen Sie den Benutzernamen fest, der für die Anmeldung beim Überwachungssystem erforderlich ist.
- **Kennwort:** Legen Sie das Kennwort für den Benutzernamen fest, für den die Anmeldung beim Überwachungssystem erfolgen soll.
- **Protokoll:** Legen Sie HTTP oder HTTPS als Protokoll an, das Sie für die Kommunikation zwischen dem CA ARCserve Central Virtual Standby-Server und dem ESX-Serversystem (Überwachungsserver) verwenden möchten.
- **Port:** Legen Sie den Port fest, den Sie für den Datentransfer zwischen dem CA ARCserve Central Virtual Standby-Server und dem ESX-Serversystem (Überwachungsserver) verwenden möchten.
- **Überwachungsserver als Proxy für den Datentransfer verwenden:** Legen Sie diese Option fest, damit der Überwachungsserver die Konvertierungsdaten vom CA ARCserve D2D-Quellknoten zum ESX-Server-Datenspeicher kopieren kann. Wenn diese Option aktiviert ist, überträgt Virtual Standby die Konvertierungsdaten vom Quellknoten zum ESX Server-Datenspeicher mithilfe einer Fibre-Channel-Kommunikation, die für die Datenübertragung schneller ist als eine LAN-Kommunikation.

  Hinweis: Die Option "Überwachungsserver als Proxy für den Datentransfer verwenden" ist standardmäßig aktiviert. Sie können diese Option deaktivieren, um es dem CA ARCserve D2D-Quellserver zu ermöglichen, die Konvertierungsdaten direkt in den Datenspeicher im ESX Server-System zu kopieren.

Hyper-V-Systeme:

- **Virtualisierungstyp:** Klicken Sie auf "Hyper-V".

  Hinweis: Wenn Sie auf "Hyper-V" klicken, sind die Überwachungsoptionen nicht zugänglich. Die Überwachungsoptionen verhalten sich so, da der Hyper-V-Server die Rolle des Überwachungsservers übernimmt.

- **Hyper-V-Hostname:** Legen Sie den Hostnamen des Hyper-V-Systems fest.
- **Benutzername:** Legen Sie den Benutzernamen fest, der für die Anmeldung beim Hyper-V-System erforderlich ist.

  Hinweis: Das Konto, das Sie angeben, muss ein administratives Konto oder ein Konto mit administrativen Berechtigungen für das Hyper-V-System sein.

- **Kennwort:** Legen Sie das Kennwort für den Benutzernamen fest, für den die Anmeldung beim Hyper-V-System erfolgen soll.
- **Port:** Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Überwachungsserver verwenden wollen.
- **Überwachungsserver:** Legen Sie den Hostnamen des Servers fest, bei dem Sie den Status des Quellservers überwachen wollen.
- **Benutzername:** Legen Sie den Benutzernamen fest, der für die Anmeldung beim Überwachungssystem erforderlich ist.
- **Kennwort:** Legen Sie das Kennwort für den Benutzernamen fest, für den die Anmeldung beim Überwachungssystem erfolgen soll.
- **Protokoll:** Legen Sie HTTP oder HTTPS als Protokoll an, das Sie für die Kommunikation zwischen dem CA ARCserve Central Virtual Standby-Server und dem Hyper-V-Serversystem (Überwachungsserver) verwenden möchten.
- **Port:** Legen Sie den Port fest, den Sie für den Datentransfer zwischen dem CA ARCserve Central Virtual Standby-Server und dem Hyper-V-Serversystem (Überwachungsserver) verwenden möchten.

Klicken Sie auf "Virtueller Rechner".

Die Optionen für "Virtueller Rechner" werden angezeigt.

6. Vervollständigen Sie die folgenden Optionen für "Virtueller Rechner":

   VMware-Systeme:

   Wenden Sie die folgenden Optionen für virtuelle Rechner auf VMware-Systeme an:

   - **Präfix des Namens des virtuellen Rechners**: Geben Sie das Präfix an, das Sie zum Anzeigenamen des virtuellen Rechners auf dem ESX Server-System hinzufügen möchten.

     Standardwert: CAVM_

   - **VM-Ressourcenpool:** Legen Sie den Namen des Ressourcenpools fest, zu dem der Virtual Standby-Rechner gruppiert werden soll.
   - **CPU-Anzahl:** Legen Sie die minimale und maximale CPU-Anzahl an, die vom virtuellen Standby-Rechner unterstützt wird.
   - **Speicher:** Legen Sie den Gesamtwert des RAM in MB fest, der für den virtuellen Standby-Rechner zugewiesen werden soll.

     Hinweis: Der angegebene RAM-Wert muss ein Vielfaches von zwei sein.

   - **VM-Datenspeicher:** Legen Sie den Speicherort fest, an dem Sie die Konvertierungsdaten speichern möchten.
     - **Geben Sie einen Datenspeicher für alle virtuellen Datenträger an:** Ermöglicht es der Anwendung, alle Datenträger, die sich auf den virtuellen Rechner beziehen, zu einem Datenspeicher zu kopieren.
     - **Geben Sie für jeden virtuellen Datenträger einen Datenspeicher an:** Ermöglicht es der Anwendung, datenträgerbezogene Informationen für den virtuellen Rechner auf den entsprechenden Datenspeicher zu kopieren.
   - **VM-Netzwerk:** Ermöglicht es Ihnen, die NICs, die virtuellen Netzwerke und Pfade zu definieren, die das ESX Server-System verwendet, um mit virtuellen Rechnern zu kommunizieren.
     - **Geben Sie für jede NIC einen Netzwerkadaptertyp an, und verbinden Sie den Netzwerkadapter mit folgendem virtuellen Netzwerk:** Ermöglicht es Ihnen festzulegen, wie die virtuelle NIC zum virtuellen Netzwerk zugeordnet werden soll. Aktivieren Sie diese Option, wenn der virtuelle Rechner virtuelle NICs und ein virtuelles Netzwerk enthält.
     - **Geben Sie für jede NIC einen Netzwerkadaptertyp und ein virtuelles Netzwerk an**: Ermöglichen es Ihnen, den Namen des virtuellen Netzwerks festzulegen, den die NIC zur Kommunikation verwenden soll.

Hyper-V-Systeme:

Wenden Sie die folgenden Optionen für virtuelle Rechner auf Hyper-V-Systeme an:

- **VM-Grundeinstellungen:** Vervollständigen Sie folgende VM-Grundeinstellungen:
  - **Präfix des Namens des virtuellen Rechners**: Geben Sie das Präfix an, das Sie zum Anzeigenamen des virtuellen Rechners auf dem Hyper-V-System hinzufügen möchten.

    Standardwert: CAVM_

    CPU-Anzahl: Legen Sie die minimale und maximale CPU-Anzahl an, die vom virtuellen Standby-System unterstützt wird.
  - **Speicher:** Legen Sie den Gesamtwert des RAM in MB fest, der für den virtuellen Standby-Rechner zugewiesen werden soll.

    Hinweis: Der angegebene RAM-Wert muss ein Vielfaches von vier sein.
- **VM-Pfad:** Geben Sie eine der folgenden VM-Pfad-Optionen an:
  - **Geben Sie einen Pfad für alle virtuellen Datenträger an:** Geben Sie den Speicherort auf dem Hyper-V-Server an, an dem Sie die Konvertierungsdaten speichern möchten.
  - **Geben Sie für jeden virtuellen Datenträger einen Pfad an:** Geben Sie den Speicherort auf dem Hyper-V-Server an, an dem Sie die Konvertierungsdaten für jeden virtuellen Datenträger speichern möchten.

  Hinweis: CA ARCserve Central Virtual Standby unterstützt keine Erstellung virtueller Datenträger-Images (VHD-Dateien) auf komprimierten Volumes oder Volumes, die vom Dateisystem verschlüsselt werden. Wenn sich der angegebene Pfad auf komprimierten oder verschlüsselten Hyper-V-Volumes befindet, lässt Sie Virtual Standby keine Richtlinie erstellen.
- **VM-Netzwerk:** Ermöglicht es Ihnen, die NICs, die virtuellen Netzwerke und Pfade zu definieren, die der Hyper-V-Server verwendet, um mit virtuellen Rechnern zu kommunizieren. Geben Sie eine der folgenden Optionen an, und füllen Sie die erforderlichen Felder aus.
  - **Geben Sie für jede NIC einen Netzwerkadaptertyp an, und verbinden Sie den Netzwerkadapter mit folgendem virtuellen Netzwerk:** Ermöglicht es Ihnen, festzulegen, auf welche Weise die virtuelle NIC dem virtuellen Netzwerk zugeordnet werden soll. Aktivieren Sie diese Option, wenn der virtuelle Rechner virtuelle NICs und ein virtuelles Netzwerk enthält.
  - **Geben Sie für jede NIC einen Netzwerkadaptertyp und ein virtuelles Netzwerk an**: Ermöglichen es Ihnen, den Namen des virtuellen Netzwerks festzulegen, den die NIC zur Kommunikation verwenden soll.

Klicken Sie auf "Aushilfseinstellungen".

Die Optionen für "Aushilfseinstellungen" werden angezeigt.

7. Vervollständigen Sie die folgenden Optionen für "Aushilfseinstellungen":

   Wiederherstellung:

   Wählen Sie eine der folgenden Methoden:

   - **Virtuellen Rechner manuell starten:** Lässt Sie virtuelle Rechner manuell in Betrieb nehmen und bereitstellen, wenn der Quellserver fehlschlägt oder aufhört, zu kommunizieren. Geben Sie diese Option an, wenn Sie es vorziehen, die Ursache für den Fehler zu analysieren, bevor Sie die virtuellen Rechner bereitstellen und die Server dafür zulassen, als Quellserver zu fungieren.
   - **Virtuellen Rechner automatisch starten:** Lässt Sie virtuelle Rechner automatisch in Betrieb nehmen und bereitstellen, wenn der Quellserver fehlschlägt oder aufhört, zu kommunizieren. Legen Sie diese Option fest, wenn Sie die virtuellen Rechner dafür zulassen möchten, sofort als Quellserver zu fungieren, wenn die Quellserver fehlschlagen oder aufhören zu kommunizieren.

   Hinweis: "Virtuellen Rechner manuell starten" ist die Standardoption zur Wiederherstellung.

   Eigenschaften der Heartbeat-Signale:

   - **Zeitlimit**: Geben Sie die Dauer der Zeit an, die der Überwachungsserver ein Heartbeat-Signal abwarten muss, bevor er einen Wiederherstellungspunkt-Snapshot einschaltet.
   - **Häufigkeit**: Legen Sie die Häufigkeit fest, mit der der Quellserver ein Heartbeat-Signal an den Überwachungsserver sendet.

     Beispiel: Der festgelegte Häufigkeitswert ist 60. Der festgelegte Häufigkeitswert ist 10. Der Quellserver sendet Heartbeat-Signale in 10-Sekunden-Intervallen. Wenn der Überwachungsserver innerhalb von 60 Sekunden nach dem letzten entdeckten Heartbeat-Signal kein Heartbeat-Signal entdeckt, schaltet der Überwachungsserver unter Verwendung des letzten Wiederherstellungspunkt-Snapshot einen virtuellen Rechner ein.

   Klicken Sie auf die Registerkarte "Voreinstellungen".

   Die Optionen für "E-Mail-Warnmeldungen" werden angezeigt.

8. Vervollständigen Sie die folgenden Optionen für E-Mail-Warnmeldungen:

   - **Fehlendes Heartbeat-Signal für Quellrechner:** Virtual Standby sendet Warnmeldungen, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver erkennt.
   - **VM eingeschaltet für Quellrechner, der mit automatischer Einschaltung konfiguriert ist:** Virtual Standby sendet Warnmeldungen, wenn ein virtueller Rechner in Betrieb genommen wird, der so konfiguriert wurde, dass eine automatische Inbetriebnahme erfolgt, wenn kein Heartbeat-Signal entdeckt wird.
   - **Fehlendes Heartbeat-Signal für Quellrechner, der für manuelles Einschalten konfiguriert ist:** Virtual Standby sendet Warnmeldungen, wenn kein Heartbeat-Signal von einem Quellserver erkannt wird, der nicht zur automatischen Inbetriebnahme konfiguriert ist.
   - **Freier VM-Speicherplatz beträgt weniger als:** Virtual Standby sendet Warnmeldungen, wenn auf dem angegebenen Hypervisor-Pfad nicht genügend freier Speicherplatz entdeckt wird. Dies tritt auf, wenn der freie Speicherplatz weniger ist als der benutzerdefinierte Schwellenwert. Der Schwellenwert kann entweder als absoluter Wert (MB) oder als prozentualer Anteil an der Gesamtkapazität angegeben werden.
   - **Virtual Standby-Fehler/-Ausfall/-Absturz:** Virtual Standby sendet Warnmeldungen, wenn ein Fehler entdeckt wird, der während des Konvertierungsprozesses aufgetreten ist.
   - **Virtual-Standby-Erfolg:** Virtual Standby sendet Warnmeldungen, wenn festgestellt wird, dass der virtuelle Rechner erfolgreich eingeschalten wurde.
   - **Hypervisor ist nicht erreichbar:** Virtual Standby sendet Warnmeldungen, wenn festgestellt wird, dass mit dem ESX Server-System oder dem Hyper-V-System keine Kommunikation möglich ist.
   - **Lizenzfehler:** Virtual Standby sendet Warnmeldungen, wenn Lizenzierungsprobleme auf Virtual Standby-Servern, Quellservern und Überwachungsservern festgestellt werden.
   - **Virtual Standby wurde nicht erfolgreich vom Wiederherstellungspunkt-Snapshot gestartet:** Virtual Standby sendet Warnmeldungen, wenn festgestellt wird, dass ein virtueller Rechner nicht automatisch eingeschaltet wurde und die Option zur Aushilfswiederherstellung "Virtuellen Rechner automatisch starten" ausgewählt ist.

   Klicken Sie auf "Speichern".

Die Richtlinie wird gespeichert.

Zuweisen von Knoten zu Richtlinien

Um Wiederherstellungspunkt-Snapshots zu erstellen, müssen Sie Virtual Standby-Richtlinien zu den CA ARCserve D2D-Knoten zuweisen, die Sie schützen möchten.

Hinweis: Sie können nicht mehr als eine Richtlinie auf einen Knoten anwenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Virtual Standby-Server an und öffnen Sie Virtual Standby.

   Klicken Sie in der Navigationsleiste der Startseite auf "Richtlinien", um die Ansicht "Richtlinien" zu öffnen.

2. Klicken Sie in der Liste "Richtlinien" auf die Richtlinie, der Sie Knoten zuweisen möchten.

   Detaillierte Informationen über die angegebene Richtlinie wird in den Registerkarten "Richtliniendetails" und "Richtlinienzuweisung" angezeigt.

3. Klicken Sie auf die Registerkarte "Richtliniendetails", um detaillierte Informationen über die Richtlinie anzuzeigen.

   (Optional) Klicken Sie in der Symbolleiste auf "Bearbeiten", um die aktuellen Einstellungen für die Richtlinie zu bearbeiten.

   Hinweis: Weitere Informationen finden Sie unter Bearbeiten von Richtlinien (siehe Seite 60).

4. Klicken Sie auf die Registerkarte "Richtlinienzuweisung".

   Klicken Sie auf der Registerkarte "Richtlinienzuweisung" auf "Zuweisen und Zuweisung aufheben".

   Das Dialogfeld "Zuweisung der Richtlinie durchführen/aufheben" wird geöffnet.

5. Geben Sie folgende Felder im Dialogfeld "Zuweisung der Richtlinie durchführen/aufheben" an:

   - **Gruppe:** Wählen Sie den Gruppennamen aus, der die Richtlinie enthält, die Sie zuweisen möchten.
   - **Knotennamenfilter:** Lässt Sie die verfügbaren Knoten basierend auf einer Gemeinsamkeit filtern.

   Hinweis: Die Filterfelder unterstützen die Verwendung von Platzhalterzeichen.

   Beispiele:

   - Acc* lässt Sie alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt.
   - *.123 lässt Sie alle Knoten filtern, deren IP-Adresse ".123" enthält.

   Hinweis: Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

6. Führen Sie eine der folgenden Aktionen aus:

   - **Zuweisen eines Knotens:** Suchen Sie in der Liste "Verfügbare Knoten" den Knoten, den Sie der Richtlinie zuweisen möchten.

     Klicken Sie auf den einzelnen Rechtspfeil.

     Der Knoten wird aus der Liste "Verfügbare Knoten" in die Liste "Ausgewählte Knoten" verschoben.

   - **Zuweisen von Knoten:** Klicken Sie in der Liste "Verfügbare Knoten" auf den doppelten Rechtspfeil.

     Alle Knoten werden aus der Liste "Verfügbare Knoten" in die Liste "Ausgewählte Knoten" verschoben.

   Klicken Sie auf "OK".

Die Knoten werden der Richtlinie zugewiesen.

Bereitstellen von Richtlinien

Nachdem Sie eine Richtlinie erstellt haben, weisen Sie einer Richtlinie Knoten zu (siehe Seite 39) und stellen Sie die Richtlinie bereit.

Das folgende Verhalten bezieht sich auf den Richtlinienbereitstellungsprozess:

- Hinweis: Der Richtlinienbereitstellungsprozess schlägt unter folgenden Bedingungen fehl:
  - Die Windows Server 2008 Hyper-V-Rolle ist auf dem CA ARCserve D2D-Quellserver (Knoten) installiert.
  - Der CA ARCserve D2D-Quellserver wurde aus CA ARCserve Central Host-Based VM Backup importiert. Die Windows Hyper-V-Rolle ist auf dem Host-Based VM Backup-Proxy-System installiert, und das Sicherungs-Proxy-System ist als Virtual Standby-Ziel angegeben.
- CA ARCserve Central Virtual Standby kann nicht automatisch virtuelle Rechner einschalten, die von CA ARCserve Central Host-Based VM Backup-Servern hinzugefügt wurden. Wenn Sie Richtlinien, die eine Wiederherstellungsmethode enthalten, die als "Virtuellen Rechner automatisch starten" (siehe Seite 32) definiert ist, auf durch Host-Based VM Backup geschützten Knoten bereitstellen, ändert Virtual Standby den Wert der Wiederherstellungsmethode in "Virtuellen Rechner manuell starten" (siehe Seite 32).

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Virtual Standby-Server an und öffnen Sie Virtual Standby.

   Klicken Sie in der Navigationsleiste der Startseite auf "Richtlinien", um die Ansicht "Richtlinien" zu öffnen.

2. Klicken Sie in der Liste "Richtlinien" auf die Richtlinie, die Sie bereitstellen möchten.

   Detaillierte Informationen über die angegebene Richtlinie wird in den Registerkarten "Richtliniendetails" und "Richtlinienzuweisung" angezeigt.

3. Klicken Sie auf die Registerkarte "Richtliniendetails", um detaillierte Informationen über die Richtlinie anzuzeigen.

   (Optional) Klicken Sie in der Symbolleiste auf "Bearbeiten", um die aktuellen Einstellungen der Richtlinie zu bearbeiten.

   Hinweis: Weitere Informationen finden Sie unter Bearbeiten von Richtlinien (siehe Seite 60).

4. Klicken Sie auf die Registerkarte "Richtlinienzuweisung".

   Detaillierte Informationen über die Knoten, die der Richtlinie zugewiesen sind, werden angezeigt.

   (Optional) Klicken Sie in der Symbolleiste auf "Zuweisen und Zuweisung aufheben", um der Richtlinie Knoten zuzuweisen oder die Zuweisung aufzuheben.

   Hinweis: Weitere Informationen finden Sie unter Zuweisen von Knoten zu Richtlinien (siehe Seite 39) bzw. Zuweisung von Knoten zu Richtlinien aufheben (siehe Seite 67).

5. Klicken Sie in der Symbolleiste auf "Jetzt bereitstellen".

   Die Bestätigungsmeldung zu "Jetzt bereitstellen" wird angezeigt.

6. Klicken Sie auf "OK".

Die Richtlinie wird bereitgestellt.

Hinweis: Sie können den Richtlinienbereitstellungsstatus für den bestimmten Knoten auch im Fenster "Knoten" in der Spalte "Richtlinie" anzeigen.

Kapitel 4: Verwenden von CA ARCserve Central Virtual Standby

Dieses Kapitel enthält folgende Themen:

Anmelden bei CA ARCserve D2D-Knoten (siehe Seite 43)
Anmelden an Überwachungsservern (siehe Seite 44)
Aufgaben zur Wartung von Knoten (siehe Seite 45)
Aufgaben zur Verwaltung von Knotengruppen (siehe Seite 56)
Verwaltungsaufgaben zu Virtual Standby-Richtlinien (siehe Seite 59)
Konfigurationsaufgaben der Anwendung (siehe Seite 69)
Anzeigen von Protokollen (siehe Seite 76)
Links zur Navigationsleiste hinzufügen (siehe Seite 77)
Startseite von Virtual Standby (siehe Seite 78)
CA ARCserve Central Virtual Standby-Überwachungs-Aufgaben (siehe Seite 83)
So schützen Sie virtuelle Virtual Standby-Rechner (siehe Seite 105)
Wiederherstellen von Daten aus CA ARCserve D2D-Wiederherstellungspunkten (siehe Seite 107)
Wiederherstellen von Daten aus CA ARCserve D2D-Dateikopien (siehe Seite 112)
Wiederherstellen von Daten mithilfe von "Wiederherzustellende Dateien/Ordner suchen" (siehe Seite 117)
Wiederherstellen von Quellservern mithilfe von Bare-Metal-Recovery (siehe Seite 122)
Wiederherstellen von Microsoft Exchange-E-Mail-Nachrichten (siehe Seite 169)
Ändern des Server-Kommunikationsprotokolls (siehe Seite 178)

Anmelden bei CA ARCserve D2D-Knoten

Auf der Virtual Standby-Startseite können Sie sich bei CA ARCserve D2D anmelden.

So melden Sie sich bei CA ARCserve D2D-Knoten an

1. Öffnen Sie die Anwendung und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

Sie sind beim CA ARCserve D2D-Knoten angemeldet.

Hinweis: Wenn Sie sich das erste Mal beim CA ARCserve D2D-Knoten anmelden, wird möglicherweise eine HTML-Seite geöffnet, die eine Warnmeldung anzeigt. Dies kann bei Verwendung von Internet Explorer auftreten. Um dieses Problem zu lösen, schließen Sie Internet Explorer und wiederholen Sie die Schritt 3. Danach sollten Sie sich problemlos beim CA ARCserve D2D-Knoten anmelden können.

Anmelden an Überwachungsservern

Mit Virtual Standby können Sie sich direkt beim Server anmelden, der die CA ARCserve D2D-Quellknoten überwacht. Vom Überwachungsserver aus können Sie Wartungsaufgaben durchführen und Informationen über den Zustand der überwachten Quellserver anzeigen. Sie können CA ARCserve D2D-Knoten von Überwachungsservern durch folgende Symbole unterscheiden:

Überwachungsserver-Symbol:

CA ARCserve D2D-Knoten-Symbol:

So melden Sie sich auf Überwachungsservern an

1. Melden Sie sich beim Virtual Standby-Server an und öffnen Sie Virtual Standby.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Knoten".

   Der Bildschirm "Knoten" wird geöffnet.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - Wenn Sie die IP-Adresse oder den Hostnamen des Überwachungsservers kennen, suchen und klicken Sie auf den Überwachungsserver, an dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".
   - Wenn Sie die IP-Adresse oder Hostnamen des Überwachungsservers nicht kennen, durchsuchen und klicken Sie auf den CA ARCserve D2D-Knoten, auf dessen Überwachungsserver Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Beim Überwachungsserver anmelden".

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

Sie sind beim Überwachungsserver angemeldet.

Aufgaben zur Wartung von Knoten

Mit Virtual Standby können Sie verschiedene Methoden verwenden, um Knoten hinzuzufügen:

- Hinzufügen von Knoten nach IP-Adresse oder Knotennamen (siehe Seite 28)
- Importieren von Knoten aus einer Datei (siehe Seite 46).

  Hinweis: Mit dieser Methode können Sie mehrere Knoten aus einer Liste von Knoten in einer durch Kommas getrennten Datei importieren.
- Hinzufügen von Knoten von CA ARCserve Central Host-Based VM Backup-Servern (siehe Seite 48).

  Hinweis: Mit dieser Methode können Sie Knoten von virtuellen Rechnern importieren, die von der CA ARCserve Central Host-Based VM Backup-Anwendung geschützt werden.

Außerdem können Sie die folgenden Knotenverwaltungsaufgaben ausführen.

- Knoten aktualisieren (siehe Seite 51).
- Knoten löschen (siehe Seite 52).

Importieren von Knoten aus einer Datei

CA ARCserve Central Virtual Standby ermöglicht es Ihnen, mehrere Knoten aus einer Datei zu importieren. Sie können Knoten aus einer Datei mit durch Komma getrennten Werten (.txt) oder einer Tabelle (.CSV) importieren.

Mit der Anwendung können Sie bis zu 100 Knoten aus einer Datei importieren. Wenn die Datei mehr als 100 Knoten enthält, importiert die Anwendung nur die ersten 100 Knoten. Wenn mehr als 100 Knoten hinzugefügt werden müssen, importieren Sie 100 mithilfe einer Datei, und fügen Sie anschließend die verbleibenden Knoten manuell hinzu.

Hinweis: Weitere Informationen über das manuelle Hinzufügen von Knoten finden Sie unter Hinzufügen von Knoten nach IP-Adresse oder Knotennamen (siehe Seite 28).

So importieren Sie Knoten aus einer Datei

1. Melden Sie sich bei der Anwendung an.

   Wählen Sie in der Navigationsleiste auf der Startseite "Knoten" aus.

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Symbolleiste "Knoten" auf "Hinzufügen" und dann im Pop-up-Menü auf "Knoten aus Datei importieren".

   Das Dialogfeld "Knoten auswählen" wird geöffnet.

3. Klicken Sie auf "Durchsuchen", um die Datei festzulegen, die die Knoten enthält, die Sie importieren wollen.

   Hinweis: Sie können eine Datei mit durch Komma getrennten Werten (CSV) oder eine Textdatei, die durch Komma getrennte Werte enthält, festlegen.

   Klicken Sie auf "Hochladen".

   Die Knotennamen und die entsprechenden Benutzernamen werden auf dem Dialogfeld angezeigt.

4. Klicken Sie auf "Weiter".

   Das Dialogfeld "Knoten-Anmeldeinformationen" wird angezeigt.

   Wenn die Benutzernamen und angegebene Kennwörter richtig sind, wird im Feld "Bestätigt" ein grünes Häkchen angezeigt. Wenn die Benutzernamen und angegebene Kennwörter nicht richtig sind, wird im Feld "Bestätigt" ein rotes Ausrufezeichen angezeigt.

5. Wählen Sie eine der folgenden Vorgehensweisen:

   - Um die Knoten hinzuzufügen, überprüfen Sie, dass alle Benutzernamen und Kennwörter richtig sind. Um die Anmeldeinformationen für einen bestimmten Knoten zu ändern, klicken Sie auf das Feld "Knotennamen".

     Das Dialogfeld "Anmeldeinformationen validieren" öffnet sich.

     Füllen Sie im Dialogfeld "Anmeldeinformationen validieren" die erforderlichen Felder aus und klicken Sie auf "OK".

   - Um einen globalen Benutzernamen und ein Kennwort auf alle Knoten anzuwenden, füllen Sie die Felder für "Benutzernamen" und "Kennwort" aus und klicken Sie auf "Auf ausgewählte Knoten anwenden".

     Der globale Benutzername und das Kennwort werden auf alle Knoten angewendet.

   Klicken Sie auf Fertig stellen.

Die Knoten werden hinzugefügt.

Hinzufügen von Knoten von CA ARCserve Central Host-Based VM Backup-Servern

CA ARCserve Central Host-Based VM Backup ist eine Anwendung, mit der Sie virtuelle Rechner mithilfe einer Instanz von CA ARCserve D2D, die auf einem Sicherungs-Proxy-Server installiert ist, sichern können. Mit CA ARCserve Central Virtual Standby können Sie die Knoten hinzufügen, die von CA ARCserve Central Host-Based VM Backup-Servern geschützt werden, um Wiederherstellungspunkt-Snapshots für die Knoten erstellen zu können. Die virtuellen Rechner müssen über CA ARCserve D2D-Richtlinien verfügen, die mithilfe von CA ARCserve Central Host-Based VM Backup zugewiesen wurden.

Beachten Sie Folgendes:

- Mit CA ARCserve Central Virtual Standby können Sie verschiedene Methoden verwenden, um Knoten hinzuzufügen:
  - Manuelles Hinzufügen von Knoten
  - Hinzufügen von Knoten aus einer Textdatei
  - Hinzufügen von Knoten von CA ARCserve Central Host-Based VM Backup-Servern

  CA ARCserve Central Virtual Standby lässt Sie Richtlinien direkt auf Knoten anwenden, während Sie mit CA ARCserve Central Host-Based VM Backup Richtlinien auf Sicherungs-Proxy-Server anwenden. Dieses Verhalten besteht weiter, nachdem Sie Knoten von CA ARCserve Central Host-Based VM Backup-Servern hinzugefügt haben.

  Hinweis: Weitere Informationen über das Zuweisen von CA ARCserve D2D-Richtlinien zu virtuellen Rechnerknoten finden Sie im *CA ARCserve Central Host-Based VM Backup-Benutzerhandbuch*.
- Virtual Standby kann Wiederherstellungspunkt-Snapshots für Knoten, die von CA ARCserve Central Host-Based VM Backup-Servern hinzugefügt wurden, nicht automatisch einschalten. Sie können Wiederherstellungspunkt-Snapshots für Knoten, die von CA ARCserve Central Host-Based VM Backup-Servern hinzugefügt wurden, jedoch manuell einschalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Wählen Sie in der Navigationsleiste auf der Startseite "Knoten" aus.

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Kategorie "Knoten" auf "Hinzufügen" und danach im Pop-up-Menü auf "Virtuellen Rechner vom CA ARCserve Central Host-Based VM Backup-Server hinzufügen".

   Das Dialogfeld "Virtuellen Rechner vom CA ARCserve Central Host-Based VM Backup-Server hinzufügen" wird geöffnet.

3. Füllen Sie folgende Felder im Dialogfeld "Virtuellen Rechner vom CA ARCserve Central Host-Based VM Backup-Server hinzufügen" aus:

   - **Computername:** Lässt Sie die IP-Adresse oder den Namen des CA ARCserve Central Host-Based VM Backup-Servers festlegen.
   - **Benutzername:** Lässt Sie den Benutzernamen festlegen, der für die Anmeldung beim CA ARCserve Central Host-Based VM Backup-Server erforderlich ist.
   - **Kennwort:** Lässt Sie das Kennwort festlegen, das für die Anmeldung beim CA ARCserve Central Host-Based VM Backup-Server erforderlich ist.
   - **Port:** Lässt Sie die Portnummer festlegen, die die Anwendung verwenden soll, um mit dem CA ARCserve Central Host-Based VM Backup-Server zu kommunizieren.
   - **HTTPS verwenden:** Lässt Sie die Verwendung einer sicheren HTTP-Kommunikation festlegen.

   Klicken Sie auf "OK".

   Eines der folgenden Ereignisse tritt ein:

   - Wenn Sie zum ersten Mal Knoten aus diesem ESX-Server-System importieren, importiert Virtual Standby alle virtuellen Rechner, die eine CA ARCserve Central Host-Based VM Backup-Richtlinienzuweisung enthalten. Nach Abschluss des Importprozesses können Sie die Knoten im Fenster "Knoten" überprüfen.
   - Wenn Sie Knoten nicht zum ersten Mal aus diesem ESX-Server-System importieren, werden im Dialogfeld "Virtuellen Rechner vom CA ARCserve Central Host-Based VM Backup-Server hinzufügen" eine Liste von Knoten angezeigt, die bereits zuvor importiert wurden. Anschließend wird ein Dialogfeld angezeigt, in dem Sie die Möglichkeit haben, Informationen der zuvor importierten Knoten zu überschreiben.
   - Wenn die Anwendung keine neuen Knoten entdeckt, wird das Dialogfeld "Virtuellen Rechner vom CA ARCserve Central Host-Based VM Backup-Server hinzufügen" geschlossen. Eine Meldung wird dann angezeigt, die Sie informiert, dass keine Knoten importiert wurden.

4. Führen Sie eine der folgenden Aktionen aus:

   - **Um die neu entdeckten Knoten hinzuzufügen und die früher entdeckten Knoten zu überschreiben:** Aktivieren Sie das Kontrollkästchen neben den Knoten, die zuvor importiert wurden, und klicken Sie auf "OK".

     Die Anwendung fügt die neu entdeckten Knoten hinzu und überschreibt die früher entdeckten Knoten. Die Anwendung überschreibt nur den Status sowie die Anmeldeinformationen, die für die zuvor entdeckten Knoten angewendet wurden.

   - **Um nur die neu entdeckten Knoten hinzuzufügen (und die zuvor entdeckten Knoten nicht zu importieren und zu überschreiben):** Aktivieren Sie nicht die Kontrollkästchen neben den Knoten, die zuvor entdeckt und importiert wurden, und klicken Sie auf "OK".

     Die Anwendung fügt nur die neu entdeckten Knoten hinzu. Die Anwendung überschreibt die zuvor entdeckten Knoten nicht.

   - **Um abzubrechen, ohne neu entdeckte Knoten oder früher entdeckte Knoten hinzuzufügen:** Klicken Sie auf "Abbrechen".

     Die Anwendung fügt keine Knoten hinzu.

5. (Optional) Klicken Sie auf der Symbolleiste auf "Aktualisieren", um zu sicherzustellen, dass alle neu hinzugefügten Knoten in der Knotenliste angezeigt werden.

Die Knoten werden hinzugefügt.

Hinweis: Wenn CA ARCserve D2D-Informationen auf dem CA ARCserve Central Host-Based VM Backup-Server aktualisiert werden, informiert der Server automatisch CA ARCserve Central Virtual Standby, um die virtuellen Rechner aus CA ARCserve Central Host-Based VM Backup zu importieren und die Richtlinien erneut bereitzustellen. Wenn CA ARCserve Central Virtual Standby nicht verfügbar ist, können Sie die virtuellen Rechner aus CA ARCserve Central Host-Based VM Backup manuell importieren.

Aktualisieren von Knoten

Mit Virtual Standby können Sie Informationen über zuvor hinzugefügte Knoten aktualisieren.

Hinweis: Sie können Knoten, die aus einem CA ARCserve Central Host-Based VM Backup-Server importiert wurden, nicht aktualisieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Wählen Sie in der Navigationsleiste auf der Startseite "Knoten" aus.

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Menüleiste "Gruppen" auf die Gruppe "Alle Knoten" oder klicken Sie auf den Gruppennamen, der die Knoten enthält, die Sie aktualisieren wollen.

   Die der Gruppe zugeordneten Knoten werden in der Knotenliste angezeigt.

3. Klicken Sie auf die Knoten, die Sie aktualisieren möchten, und klicken Sie anschließend mit der rechten Maustaste, und wählen Sie im Pop-up-Menü die Option "Knoten aktualisieren".

   Das Dialogfeld "Knoten aktualisieren" wird geöffnet.

   Hinweis: Um alle Knoten in der Knotengruppe zu aktualisieren, klicken Sie mit der rechten Maustaste auf den Namen "Knotengruppe", und klicken Sie anschließend im Pop-up-Menü auf "Knoten aktualisieren".

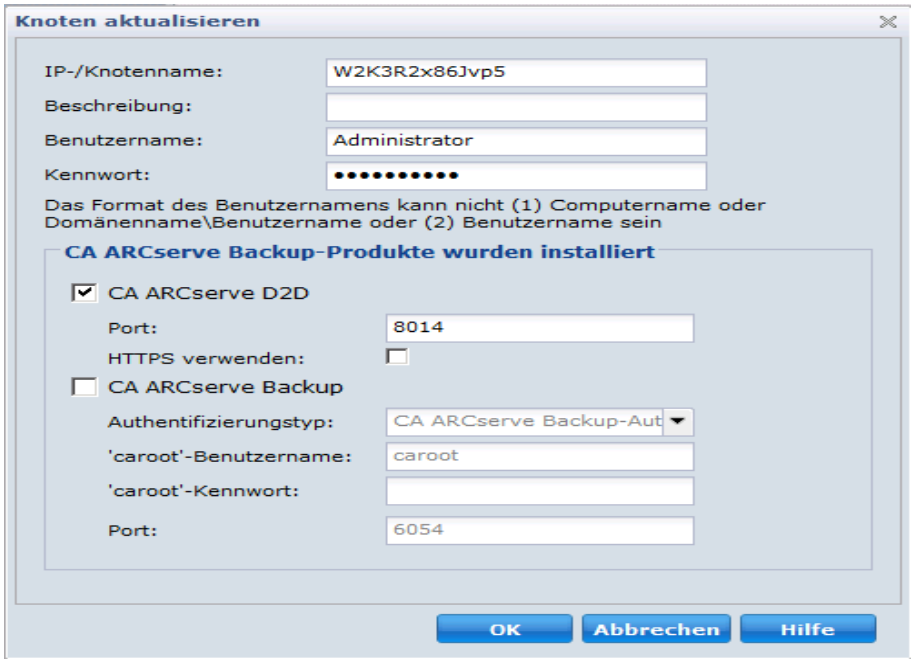
4. Aktualisieren Sie die Knotendetails nach Bedarf.

   Hinweis: Um mehrere Knoten mit der rechten Maustaste auf der Knotenliste zu aktualisieren, wählen Sie die gewünschten Knoten aus, klicken Sie mit der rechten Maustaste auf einen Knoten, und klicken Sie dann im Pop-up-Menü auf "Aktualisieren". Benutzername und Kennwort sind für alle ausgewählten Knoten gleich. Standardmäßig sind die Option "Neue Anmeldeinformationen angeben" und das Kontrollkästchen "Steuerung übernehmen für Knoten" aktiviert. Sie können einen neuen Benutzernamen und Kennwort für die ausgewählten Knoten angeben und können diesen Server zwingen, die Knoten zu verwalten. Außerdem können Sie die Option "Vorhandene Anmeldeinformationen verwenden", um den aktuellen Benutzernamen und das aktuelle Kennwort anzuwenden. Die Felder werden deaktiviert.

5. Klicken Sie auf "OK".

   Das Dialogfeld "Knoten aktualisieren" wird geschlossen, und die Knoten werden aktualisiert.

   Hinweis: Wenn an CA ARCserve D2D-Knoten Änderungen vorgenommen wurden, öffnet sich das Dialogfeld "Knoten aktualisieren", damit Sie weitere Details angeben können.



6. (Optional) Wenn die aktualisierten Informationen nicht in der Knotenliste anzeigt werden, klicken Sie in der Symbolleiste auf "Aktualisieren".

Der Knoten wird aktualisiert.

Löschen von Knoten

Mit Virtual Standby können Sie Knoten aus Ihrer Umgebung löschen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie in der Menüleiste "Gruppen" auf die Gruppe "Alle Knoten" oder klicken Sie auf den Gruppennamen, der den Knoten enthält, den Sie löschen wollen.

   Die der Gruppe zugeordneten Knoten werden in der Knotenliste angezeigt.

3. Markieren Sie einen oder mehrere Knoten, die Sie löschen wollen, und klicken Sie dann in der Symbolleiste auf "Löschen".

   Eine Bestätigungsmeldung wird angezeigt.

4. Wählen Sie eine der folgenden Vorgehensweisen:

   - Klicken Sie auf "Ja", um den Knoten zu löschen.

Klicken Sie auf "Nein", wenn Sie den Knoten nicht löschen wollen.

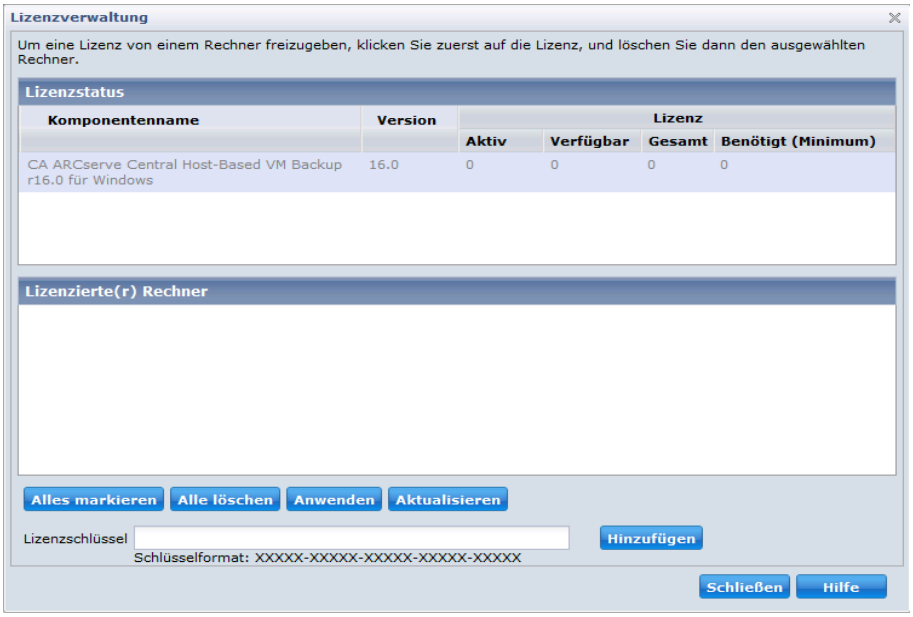
Freigeben von Lizenzen von Knoten

DieCA ARCserve Central Virtual Standby-Lizenzierung erfolgt über einen anzahlbasierten Mechanismus. Bei der anzahlbasierten Lizenzierung können Sie eine einzige Pauschallizenz für den Knoten gewähren. Diese Pauschallizenz enthält eine vorher festgelegte Anzahl aktiver Lizenzrechte, die im Gesamtlizenzbestand enthalten sind. Jedem Knoten, der die Lizenz verwendet, wird in der Reihenfolge der Anfragen eine aktive Lizenz aus dem Bestand gewährt, bis alle verfügbaren Lizenzen vergeben sind. Wenn alle aktiven Lizenzrechte angewendet wurden und Sie eine Lizenz zu einem anderen Knoten hinzufügen möchten, geben Sie die Lizenzrechte von einem oder mehreren Knoten frei, um die Anzahl verfügbarer Lizenzen zu erhöhen, damit für den andere Knoten verfügbar wird.

So geben Sie Lizenzen von Knoten frei

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie im Startbildschirm auf "Hilfe" und "Lizenzen verwalten", um das Dialogfeld "Lizenzverwaltung" zu öffnen.

   Das Dialogfeld "Lizenzverwaltung" wird geöffnet und zeigt, wir in der folgenden Abbildung veranschaulicht, eine Liste der Lizenzen an, die auf physische Computer, VMware-basierte virtuelle Rechner und Hyper-V-basierte virtuelle Rechner angewendet sind:



3. Wählen Sie im Abschnitt "Lizenzstatus" die Lizenz aus, die Sie von Knoten freigeben möchten.

   Die Knoten, die die Lizenz verwenden, werden im Abschnitt "Lizenzierte(r) Rechner" des Dialogfelds "Lizenzverwaltung" angezeigt.

4. Aktivieren Sie das Kontrollkästchen neben den Knoten, deren Lizenzen freigegeben werden sollen.

   Hinweis: Klicken Sie auf "Alle löschen", um das Kontrollkästchen neben allen Knoten zu deaktivieren, die im Abschnitt "Lizenzierte(r) Rechner" des Dialogfelds "Lizenzverwaltung" angezeigt werden.

5. Klicken Sie auf "Übernehmen".

   Die Lizenz wird vom angegebenen Knoten freigegeben.

6. (Optional) Klicken Sie auf "Aktualisieren", um die Knotenliste mit der angegebenen Lizenz zu aktualisieren.

Überwachen von Knoten über den Überwachungsserver beenden

CA ARCserve Central Virtual Standby ermöglicht es Ihnen, die Überwachung von Knoten auf der Registerkarte "Virtual Standby" auf dem Überwachungsserver zu beenden.

Wichtig! Wenn Sie die Überwachung von Knoten beenden, dürfen die virtuellen Virtual Standby-Rechner nicht die aktuellsten Wiederherstellungspunkt-Snapshots enthalten, die für das Einschalten der virtuellen Rechner erforderlich sind. Außerdem können Sie nur vom Hypervisor-System aus virtuelle Rechner für die Knoten einschalten, für die Sie die Überwachung (manuell) beendet haben.

So beenden Sie die Überwachung der Knoten über den Überwachungsserver

1. Melden Sie sich auf dem Überwachungsserver an.

   Hinweis: Weitere Informationen finden Sie unter Anmelden an Überwachungsservern (siehe Seite 44).

2. Wenn der Überwachungsserver geöffnet ist, klicken Sie auf die Registerkarte "Virtual Standby".

   Das Fenster "Virtual Standby" wird geöffnet.

3. Erweitern Sie in der Baumstruktur "Quellen" die Felder "Alle", "Quelle wird ausgeführt", "Aktion erforderlich" oder "VM wird ausgeführt", um den Quellknoten zu finden, dessen Überwachung Sie beenden möchten.

4. Klicken Sie mit der rechten Maustaste auf den Knoten, dessen Überwachung Sie beenden möchten, und klicken Sie im Pop-up-Menü auf "Monitoring anhalten".

   Eine Warnmeldung wird angezeigt.

5. Wenn Sie sicher sind, dass Sie die Überwachung des angegebenen Knotens beenden möchten, klicken Sie auf "Ja".

Der Knoten wird aus der Baumstruktur "Quellen" entfernt, und der Überwachungsserver beendet die Überwachung des Knotens.

Aktualisieren von Knoten und Richtlinien nach einer Änderung des Hostnamens des CA ARCserve Central Applications-Servers

Wenn Sie den Hostnamen des CA ARCserve Central Virtual Standby-Servers geändert haben, aktualisieren Sie die Knoten und die Richtlinien, die auf die Knoten angewendet werden. Sie führen diese Aufgaben aus, um die Beziehung zwischen dem CA ARCserve Central Virtual Standby-Server und den Knoten, die der CA ARCserve Central Virtual Standby-Server schützt, zu verwalten. In der folgenden Tabelle sind die möglichen Szenarien sowie die entsprechenden Korrekturmaßnahmen beschrieben.

Szenario	Korrekturmaßnahme
Der Knoten wurde hinzugefügt, nachdem der Hostname des CA ARCserve Central Virtual Standby-Servers geändert wurde.	Es ist keine Aktion erforderlich.
Der Knoten wurde hinzugefügt, bevor der Hostname des CA ARCserve Central Virtual Standby-Servers geändert wurde, und eine Richtlinie wurde nicht auf den Knoten angewandt.	Aktualisieren Sie den Knoten. Weitere Informationen finden Sie unter Aktualisieren von Knoten (siehe Seite 51).
Der Knoten wurde hinzugefügt, bevor der Hostname des CA ARCserve Central Virtual Standby-Servers geändert wurde, und eine Richtlinie wurde auf den Knoten angewandt.	Wenden Sie die Richtlinie erneut an. Weitere Informationen finden Sie unter Bereitstellen von Richtlinien (siehe Seite 40).

Aufgaben zur Verwaltung von Knotengruppen

Mit Virtual Standby können Sie die von Ihnen geschützten CA ARCserve D2D-Knotengruppen verwalten.

Dieser Abschnitt enthält folgende Themen:

Ändern von Knotengruppen (siehe Seite 57)
Löschen von Knotengruppen (siehe Seite 58)
Filtern von Knotengruppen (siehe Seite 59)

Ändern von Knotengruppen

Die Anwendung lässt Sie die Knotengruppen ändern, die Sie erstellt haben. Sie können Knoten zu Knotengruppen hinzufügen und aus ihnen entfernen und den Namen von Knotengruppen ändern.

Hinweis: Sie können folgende Knotengruppen nicht ändern:

- **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
- **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
- **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
- **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten und Microsoft SQL Server ist installiert.
- **Exchange:** Enthält alle der Anwendung zugeordneten Knoten und Microsoft SQL Server ist installiert.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie auf die Knotengruppe, die Sie ändern wollen, und dann in der Symbolleiste der Knotengruppe auf "Ändern".

   Das Dialogfeld "Gruppe ändern" wird geöffnet.

3. Um den Gruppennamen zu ändern, geben Sie einen neuen Namen im Feld "Gruppennamen" an.

4. Um Knoten zur Knotengruppe hinzuzufügen, wählen Sie die Knoten aus, die Sie zur Knotengruppe hinzufügen möchten, und klicken Sie auf den Rechtspfeil.

   Die Knoten verschieben sich von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" und werden der Knotengruppe zugewiesen.

   Hinweis: Um alle Knoten von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" zu verschieben, klicken Sie auf den doppelten Rechtspfeil.

5. Um Knoten aus der Knotengruppe zu entfernen, klicken Sie auf den linken Pfeil, um einen, oder auf den doppelten Linkspfeil, um alle Knoten zu entfernen.

6. (Optional) Um die verfügbaren Knoten basierend auf einer Gemeinsamkeit zu filtern, legen Sie im Feld "Knotennamenfilter" einen Filterwert fest.

   Hinweis: Das Feld "Filter" unterstützt die Verwendung von Platzhalterzeichen.

   Acc* lässt Sie beispielsweise alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt. Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

7. Klicken Sie auf "OK".

Die Knotengruppe wird geändert.

Löschen von Knotengruppen

Die Anwendung lässt Sie die Knotengruppen löschen, die Sie erstellt haben.

Sie können folgende Knotengruppen nicht löschen:

- **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
- **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
- **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
- **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft SQL Server ist auf dem Knoten installiert.
- **Exchange:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft Exchange Server ist auf dem Knoten installiert.

Hinweis: Das Löschen von Knotengruppen löscht keine individuelle Knoten aus der Anwendung.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie auf die Knotengruppe, die Sie löschen wollen, und dann in der Symbolleiste der Knotengruppe auf "Löschen".

   Das Meldungsdialogfeld "Bestätigen" öffnet sich.

3. Wenn Sie sicher sind, dass Sie die Knotengruppe löschen möchten, klicken Sie auf "Ja".

   Hinweis: Klicken Sie auf "Nein", wenn Sie die Knotengruppe nicht löschen wollen.

Die Knotengruppe wird gelöscht.

Filtern von Knotengruppen

Virtual Standby lässt Sie Filter verwenden, um CA ARCserve D2D-Knoten in einer Gruppe anzuzeigen, auf der eine bestimmte Anwendung installiert ist. Mit Virtual Standby können Sie die Knoten filtern, auf denen folgende Anwendungen installiert sind:

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

So filtern Sie Knotengruppen

1. Melden Sie sich beim Virtual Standby-Server an und öffnen Sie Virtual Standby.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt:

2. Klicken Sie in der Liste "Gruppen" auf die Gruppe, die Sie filtern möchten.

   Hinweis: Sie können alle Standardgruppen (Alle Knoten, Nicht zugewiesen, SQL Server und Exchange) und alle individuell benannten Gruppen filtern.

   Klicken Sie in der Symbolleiste "Filter" auf das Kontrollkästchen neben der Anwendung, die Sie filtern möchten.

Die Knotengruppe wird gefiltert.

Verwaltungsaufgaben zu Virtual Standby-Richtlinien

Virtual Standby ermöglicht es Ihnen, die Konvertierungsrichtlinien zu verwalten, die Sie verwenden, um Ihre CA ARCserve D2D-Knoten zu schützen.

Dieser Abschnitt enthält folgende Themen:

Bearbeiten oder Kopieren von Richtlinien (siehe Seite 60)
Zuweisung von Knoten zu Richtlinien aufheben (siehe Seite 67)
Löschen von Richtlinien (siehe Seite 68)

Bearbeiten oder Kopieren von Richtlinien

Mit Virtual Standby können Sie Richtlinien bearbeiten oder kopieren, nachdem sie erstellt wurden.

So bearbeiten Sie Richtlinien

1. Melden Sie sich beim Virtual Standby-Server an und öffnen Sie Virtual Standby.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Richtlinien".

   Das Fenster "Richtlinien" wird geöffnet.

2. Klicken Sie im Fenster "Richtlinien" auf das Kontrollkästchen neben einer Richtlinie und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie in der Symbolleiste auf "Bearbeiten" und bearbeiten Sie die ausgewählte Richtlinie.
   - Klicken Sie in der Symbolleiste auf "Kopieren", um eine Richtlinie der ausgewählten Richtlinie zu kopieren und neu zu erstellen.

     Hinweis: Wenn Sie eine Richtlinie kopieren, öffnet sich das Dialogfeld "Richtlinie kopieren". Geben Sie einen Namen für die neue Richtlinie ein, und klicken Sie auf "OK".

   Das Dialogfeld "Richtlinie bearbeiten" wird geöffnet.

3. Wenn Sie den Namen der Richtlinie ändern wollen, geben Sie einen Namen im Feld "Richtliniennamen" an.
4. Klicken Sie auf die Registerkarte "Virtual Standby".

   Die Optionen "Virtualisierungsserver", "Virtueller Rechner" und "Aushilfseinstellungen" werden angezeigt.

5. Klicken Sie auf "Virtualisierungsserver".

   Die Optionen für "Virtualisierungsserver" werden angezeigt.

6. Vervollständigen Sie die folgenden Optionen für "Virtualisierungsserver":

   VMware-Systeme:

   - **Virtualisierungstyp:** Klicken Sie auf "VMware".
   - **ESX-Host/-Virtual Center**: Legen Sie den Hostnamen des ESX- oder vCenter Server-Systems fest.
   - **Benutzername:** Legen Sie den Benutzernamen fest, der für die Anmeldung beim VMware-System erforderlich ist.

     Hinweis: Das Konto, das Sie angeben, muss ein administratives Konto oder ein Konto mit administrativen Berechtigungen für das ESX- oder vCenter Server-System sein.

- **Kennwort:** Legen Sie das Kennwort für den Benutzernamen fest, für den die Anmeldung beim VMware-System erfolgen soll.
- **Protokoll:** Legen Sie HTTP oder HTTPS als Protokoll an, das Sie für die Kommunikation zwischen dem CA ARCserve D2D-Quellknoten und dem Überwachungsserver verwenden möchten.
- **Port:** Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Überwachungsserver verwenden wollen.
- **ESX-Knoten:** Die Werte in diesem Feld variieren basierend auf dem Wert, der im Feld "ESX-Host/vCenter" angegeben wird:
  - **ESX Server-Systeme:** Wenn Sie ein ESX Server-System im Feld "ESX-Host/vCenter" angeben, zeigt dieses Feld den Hostnamen des ESX Server-Systems an.
  - **vCenter Server-Systeme:** Wenn Sie ein vCenter Server-System im Feld "ESX-Host/vCenter" angeben, können Sie in diesem Feld (aus einer Drop-down-Liste) das ESX Server-System angeben, das Sie mit dieser Richtlinie verknüpfen möchten.
- **Überwachungsserver:** Legen Sie den Hostnamen des Servers fest, bei dem Sie den Status des Quellservers überwachen wollen.

  Hinweis: Der Überwachungsserver kann ein beliebiger physischer Computer oder virtueller Rechner sein, vorausgesetzt, dass er kein Proxy-Server für eine CA ARCserve Central Host-Based VM Backup-Implementierung ist.
- **Benutzername:** Legen Sie den Benutzernamen fest, der für die Anmeldung beim Überwachungssystem erforderlich ist.
- **Kennwort:** Legen Sie das Kennwort für den Benutzernamen fest, für den die Anmeldung beim Überwachungssystem erfolgen soll.
- **Protokoll:** Legen Sie HTTP oder HTTPS als Protokoll an, das Sie für die Kommunikation zwischen dem CA ARCserve Central Virtual Standby-Server und dem ESX-Serversystem (Überwachungsserver) verwenden möchten.
- **Port:** Legen Sie den Port fest, den Sie für den Datentransfer zwischen dem CA ARCserve Central Virtual Standby-Server und dem ESX-Serversystem (Überwachungsserver) verwenden möchten.
- **Überwachungsserver als Proxy für den Datentransfer verwenden:** Legen Sie diese Option fest, damit der Überwachungsserver die Konvertierungsdaten vom CA ARCserve D2D-Quellknoten zum ESX-Server-Datenspeicher kopieren kann. Wenn diese Option aktiviert ist, überträgt Virtual Standby die Konvertierungsdaten vom Quellknoten zum ESX Server-Datenspeicher mithilfe einer Fibre-Channel-Kommunikation, die für die Datenübertragung schneller ist als eine LAN-Kommunikation.

Hinweis: Die Option "Überwachungsserver als Proxy für den Datentransfer verwenden" ist standardmäßig aktiviert. Sie können diese Option deaktivieren, um es dem CA ARCserve D2D-Quellserver zu ermöglichen, die Konvertierungsdaten direkt in den Datenspeicher im ESX Server-System zu kopieren.

Hyper-V-Systeme:

- **Virtualisierungstyp:** Klicken Sie auf "Hyper-V".

  Hinweis: Wenn Sie auf "Hyper-V" klicken, sind die Überwachungsoptionen nicht zugänglich. Die Überwachungsoptionen verhalten sich so, da der Hyper-V-Server die Rolle des Überwachungsservers übernimmt.

- **Hyper-V-Hostname:** Legen Sie den Hostnamen des Hyper-V-Systems fest.
- **Benutzername:** Legen Sie den Benutzernamen fest, der für die Anmeldung beim Hyper-V-System erforderlich ist.

  Hinweis: Das Konto, das Sie angeben, muss ein administratives Konto oder ein Konto mit administrativen Berechtigungen für das Hyper-V-System sein.

- **Kennwort:** Legen Sie das Kennwort für den Benutzernamen fest, für den die Anmeldung beim Hyper-V-System erfolgen soll.
- **Port:** Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Überwachungsserver verwenden wollen.
- **Überwachungsserver:** Legen Sie den Hostnamen des Servers fest, bei dem Sie den Status des Quellservers überwachen wollen.
- **Benutzername:** Legen Sie den Benutzernamen fest, der für die Anmeldung beim Überwachungssystem erforderlich ist.
- **Kennwort:** Legen Sie das Kennwort für den Benutzernamen fest, für den die Anmeldung beim Überwachungssystem erfolgen soll.
- **Protokoll:** Legen Sie HTTP oder HTTPS als Protokoll an, das Sie für die Kommunikation zwischen dem CA ARCserve Central Virtual Standby-Server und dem Hyper-V-Serversystem (Überwachungsserver) verwenden möchten.
- **Port:** Legen Sie den Port fest, den Sie für den Datentransfer zwischen dem CA ARCserve Central Virtual Standby-Server und dem Hyper-V-Serversystem (Überwachungsserver) verwenden möchten.

Klicken Sie auf "Virtueller Rechner".

Die Optionen für "Virtueller Rechner" werden angezeigt.

7. Vervollständigen Sie die folgenden Optionen für "Virtueller Rechner":

   VMware-Systeme:

   Wenden Sie die folgenden Optionen für virtuelle Rechner auf VMware-Systeme an:

   - **Präfix des Namens des virtuellen Rechners**: Geben Sie das Präfix an, das Sie zum Anzeigenamen des virtuellen Rechners auf dem ESX Server-System hinzufügen möchten.

     Standardwert: CAVM_

   - **VM-Ressourcenpool:** Legen Sie den Namen des Ressourcenpools fest, zu dem der Virtual Standby-Rechner gruppiert werden soll.
   - **CPU-Anzahl:** Legen Sie die minimale und maximale CPU-Anzahl an, die vom virtuellen Standby-Rechner unterstützt wird.
   - **Speicher:** Legen Sie den Gesamtwert des RAM in MB fest, der für den virtuellen Standby-Rechner zugewiesen werden soll.

     Hinweis: Der angegebene RAM-Wert muss ein Vielfaches von zwei sein.

   - **VM-Datenspeicher:** Legen Sie den Speicherort fest, an dem Sie die Konvertierungsdaten speichern möchten.
     - **Geben Sie einen Datenspeicher für alle virtuellen Datenträger an:** Ermöglicht es der Anwendung, alle Datenträger, die sich auf den virtuellen Rechner beziehen, zu einem Datenspeicher zu kopieren.
     - **Geben Sie für jeden virtuellen Datenträger einen Datenspeicher an:** Ermöglicht es der Anwendung, datenträgerbezogene Informationen für den virtuellen Rechner auf den entsprechenden Datenspeicher zu kopieren.
   - **VM-Netzwerk:** Ermöglicht es Ihnen, die NICs, die virtuellen Netzwerke und Pfade zu definieren, die das ESX Server-System verwendet, um mit virtuellen Rechnern zu kommunizieren.
     - **Geben Sie für jede NIC einen Netzwerkadaptertyp an, und verbinden Sie den Netzwerkadapter mit folgendem virtuellen Netzwerk:** Ermöglicht es Ihnen festzulegen, wie die virtuelle NIC zum virtuellen Netzwerk zugeordnet werden soll. Aktivieren Sie diese Option, wenn der virtuelle Rechner virtuelle NICs und ein virtuelles Netzwerk enthält.
     - **Geben Sie für jede NIC einen Netzwerkadaptertyp und ein virtuelles Netzwerk an**: Ermöglichen es Ihnen, den Namen des virtuellen Netzwerks festzulegen, den die NIC zur Kommunikation verwenden soll.

Hyper-V-Systeme:

Wenden Sie die folgenden Optionen für virtuelle Rechner auf Hyper-V-Systeme an:

- **VM-Grundeinstellungen:** Vervollständigen Sie folgende VM-Grundeinstellungen:
  - **Präfix des Namens des virtuellen Rechners**: Geben Sie das Präfix an, das Sie zum Anzeigenamen des virtuellen Rechners auf dem Hyper-V-System hinzufügen möchten.

    Standardwert: CAVM_

    CPU-Anzahl: Legen Sie die minimale und maximale CPU-Anzahl an, die vom virtuellen Standby-System unterstützt wird.
  - **Speicher:** Legen Sie den Gesamtwert des RAM in MB fest, der für den virtuellen Standby-Rechner zugewiesen werden soll.

    Hinweis: Der angegebene RAM-Wert muss ein Vielfaches von vier sein.
- **VM-Pfad:** Geben Sie eine der folgenden VM-Pfad-Optionen an:
  - **Geben Sie einen Pfad für alle virtuellen Datenträger an:** Geben Sie den Speicherort auf dem Hyper-V-Server an, an dem Sie die Konvertierungsdaten speichern möchten.
  - **Geben Sie für jeden virtuellen Datenträger einen Pfad an:** Geben Sie den Speicherort auf dem Hyper-V-Server an, an dem Sie die Konvertierungsdaten für jeden virtuellen Datenträger speichern möchten.

  Hinweis: CA ARCserve Central Virtual Standby unterstützt keine Erstellung virtueller Datenträger-Images (VHD-Dateien) auf komprimierten Volumes oder Volumes, die vom Dateisystem verschlüsselt werden. Wenn sich der angegebene Pfad auf komprimierten oder verschlüsselten Hyper-V-Volumes befindet, lässt Sie Virtual Standby keine Richtlinie erstellen.
- **VM-Netzwerk:** Ermöglicht es Ihnen, die NICs, die virtuellen Netzwerke und Pfade zu definieren, die der Hyper-V-Server verwendet, um mit virtuellen Rechnern zu kommunizieren. Geben Sie eine der folgenden Optionen an, und füllen Sie die erforderlichen Felder aus.
  - **Geben Sie für jede NIC einen Netzwerkadaptertyp an, und verbinden Sie den Netzwerkadapter mit folgendem virtuellen Netzwerk:** Ermöglicht es Ihnen, festzulegen, auf welche Weise die virtuelle NIC dem virtuellen Netzwerk zugeordnet werden soll. Aktivieren Sie diese Option, wenn der virtuelle Rechner virtuelle NICs und ein virtuelles Netzwerk enthält.
  - **Geben Sie für jede NIC einen Netzwerkadaptertyp und ein virtuelles Netzwerk an**: Ermöglichen es Ihnen, den Namen des virtuellen Netzwerks festzulegen, den die NIC zur Kommunikation verwenden soll.

Klicken Sie auf "Aushilfseinstellungen".

Die Optionen für "Aushilfseinstellungen" werden angezeigt.

8. Vervollständigen Sie die folgenden Optionen für "Aushilfseinstellungen":

   Wiederherstellung:

   Wählen Sie eine der folgenden Methoden:

   - **Virtuellen Rechner manuell starten:** Lässt Sie virtuelle Rechner manuell in Betrieb nehmen und bereitstellen, wenn der Quellserver fehlschlägt oder aufhört, zu kommunizieren. Geben Sie diese Option an, wenn Sie es vorziehen, die Ursache für den Fehler zu analysieren, bevor Sie die virtuellen Rechner bereitstellen und die Server dafür zulassen, als Quellserver zu fungieren.
   - **Virtuellen Rechner automatisch starten:** Lässt Sie virtuelle Rechner automatisch in Betrieb nehmen und bereitstellen, wenn der Quellserver fehlschlägt oder aufhört, zu kommunizieren. Legen Sie diese Option fest, wenn Sie die virtuellen Rechner dafür zulassen möchten, sofort als Quellserver zu fungieren, wenn die Quellserver fehlschlagen oder aufhören zu kommunizieren.

   Hinweis: "Virtuellen Rechner manuell starten" ist die Standardoption zur Wiederherstellung.

   Eigenschaften der Heartbeat-Signale:

   - **Zeitlimit**: Geben Sie die Dauer der Zeit an, die der Überwachungsserver ein Heartbeat-Signal abwarten muss, bevor er einen Wiederherstellungspunkt-Snapshot einschaltet.
   - **Häufigkeit**: Legen Sie die Häufigkeit fest, mit der der Quellserver ein Heartbeat-Signal an den Überwachungsserver sendet.

     Beispiel: Der festgelegte Häufigkeitswert ist 60. Der festgelegte Häufigkeitswert ist 10. Der Quellserver sendet Heartbeat-Signale in 10-Sekunden-Intervallen. Wenn der Überwachungsserver innerhalb von 60 Sekunden nach dem letzten entdeckten Heartbeat-Signal kein Heartbeat-Signal entdeckt, schaltet der Überwachungsserver unter Verwendung des letzten Wiederherstellungspunkt-Snapshot einen virtuellen Rechner ein.

   Klicken Sie auf die Registerkarte "Voreinstellungen".

   Die Optionen für "E-Mail-Warnmeldungen" werden angezeigt.

9. Vervollständigen Sie die folgenden Optionen für E-Mail-Warnmeldungen:

   - **Fehlendes Heartbeat-Signal für Quellrechner:** Virtual Standby sendet Warnmeldungen, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver erkennt.
   - **VM eingeschaltet für Quellrechner, der mit automatischer Einschaltung konfiguriert ist:** Virtual Standby sendet Warnmeldungen, wenn ein virtueller Rechner in Betrieb genommen wird, der so konfiguriert wurde, dass eine automatische Inbetriebnahme erfolgt, wenn kein Heartbeat-Signal entdeckt wird.
   - **Fehlendes Heartbeat-Signal für Quellrechner, der für manuelles Einschalten konfiguriert ist:** Virtual Standby sendet Warnmeldungen, wenn kein Heartbeat-Signal von einem Quellserver erkannt wird, der nicht zur automatischen Inbetriebnahme konfiguriert ist.
   - **Freier VM-Speicherplatz beträgt weniger als:** Virtual Standby sendet Warnmeldungen, wenn auf dem angegebenen Hypervisor-Pfad nicht genügend freier Speicherplatz entdeckt wird. Dies tritt auf, wenn der freie Speicherplatz weniger ist als der benutzerdefinierte Schwellenwert. Der Schwellenwert kann entweder als absoluter Wert (MB) oder als prozentualer Anteil an der Gesamtkapazität angegeben werden.
   - **Virtual Standby-Fehler/-Ausfall/-Absturz:** Virtual Standby sendet Warnmeldungen, wenn ein Fehler entdeckt wird, der während des Konvertierungsprozesses aufgetreten ist.
   - **Virtual-Standby-Erfolg:** Virtual Standby sendet Warnmeldungen, wenn festgestellt wird, dass der virtuelle Rechner erfolgreich eingeschalten wurde.
   - **Hypervisor ist nicht erreichbar:** Virtual Standby sendet Warnmeldungen, wenn festgestellt wird, dass mit dem ESX Server-System oder dem Hyper-V-System keine Kommunikation möglich ist.
   - **Lizenzfehler:** Virtual Standby sendet Warnmeldungen, wenn Lizenzierungsprobleme auf Virtual Standby-Servern, Quellservern und Überwachungsservern festgestellt werden.
   - **Virtual Standby wurde nicht erfolgreich vom Wiederherstellungspunkt-Snapshot gestartet:** Virtual Standby sendet Warnmeldungen, wenn festgestellt wird, dass ein virtueller Rechner nicht automatisch eingeschaltet wurde und die Option zur Aushilfswiederherstellung "Virtuellen Rechner automatisch starten" ausgewählt ist.

   Klicken Sie auf "Speichern".

Die Richtlinie wird bearbeitet.

Zuweisung von Knoten zu Richtlinien aufheben

Virtual Standby ermöglicht es Ihnen, die Zuweisung von Knoten zu Richtlinien aufzuheben. Mit Virtual Standby können Sie nicht mehrere Richtlinien zu Knoten zuweisen. Wenn Sie Knoten zu neuen Richtlinien zuweisen möchten, müssen Sie die Zuweisung der aktuellen Richtlinie der Knoten aufheben, bevor Sie den Knoten eine neue Richtlinie zuweisen können.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Virtual Standby-Server an und öffnen Sie Virtual Standby.

   Klicken Sie in der Navigationsleiste der Startseite auf "Richtlinien", um die Ansicht "Richtlinien" zu öffnen.

2. Klicken Sie in der Liste "Richtlinien" auf die Richtlinie, deren Zuweisung von Knoten Sie aufheben möchten.

   Detaillierte Informationen über die angegebene Richtlinie wird in den Registerkarten "Richtliniendetails" und "Richtlinienzuweisung" angezeigt.

3. Klicken Sie auf die Registerkarte "Richtliniendetails", um detaillierte Informationen über die Richtlinie anzuzeigen.

   (Optional) Klicken Sie in der Symbolleiste "Richtlinien" auf "Bearbeiten", um die aktuellen Einstellungen der Richtlinie zu bearbeiten.

   Hinweis: Weitere Informationen finden Sie unter Bearbeiten von Richtlinien (siehe Seite 60).

4. Klicken Sie auf die Registerkarte "Richtlinienzuweisung".

   Klicken Sie auf der Registerkarte "Richtlinienzuweisung" auf die Option "Zuweisen und Zuweisung aufheben", um das Dialogfeld "Zuweisung der Richtlinie durchführen/aufheben" zu öffnen.

5. Geben Sie folgende Felder im Dialogfeld "Zuweisung der Richtlinie durchführen/aufheben" an:

   - **Gruppe:** Wählen Sie den Gruppennamen aus, der die Richtlinie enthält, die Sie zuweisen möchten.
   - **Knotennamenfilter:** Lässt Sie die verfügbaren Knoten basierend auf einer Gemeinsamkeit filtern.

   Hinweis: Die Filterfelder unterstützen die Verwendung von Platzhalterzeichen.

   Beispiele:

   - Acc* lässt Sie alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt.
   - *.123 lässt Sie alle Knoten filtern, deren IP-Adresse ".123" enthält.

   Hinweis: Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

6. Führen Sie eine der folgenden Aktionen aus:

   - **Aufheben der Zuweisung eines Knotens:** Suchen Sie in der Liste "Ausgewählte Knoten" den Knoten, für den Sie die Zuweisung der Richtlinie aufheben möchten.

     Klicken Sie auf den einzelnen Linkspfeil.

     Der Knoten wird aus der Liste "Ausgewählte Knoten" in die Liste "Verfügbare Knoten" verschoben.

   - **Aufheben der Zuweisung von Knoten:** Klicken Sie in der Liste "Ausgewählte Knoten" auf den doppelten Linkspfeil.

     Alle Knoten werden aus der Liste "Ausgewählte Knoten" in die Liste "Verfügbare Knoten" verschoben.

   Klicken Sie auf "OK".

Die Zuweisung der Knoten zur Richtlinie wird aufgehoben.

Löschen von Richtlinien

Mit Virtual Standby können Sie Richtlinien löschen, die zuvor erstellt wurden.

Hinweis: Mit Virtual Standby können Sie keine Richtlinien löschen, die Knoten zugewiesen sind. Um Richtlinien mit zugewiesenen Knoten zu löschen, müssen Sie die Zuweisung der Knoten zur Richtlinie aufheben und anschließend die Richtlinie löschen. Weitere Informationen darüber, wie Zuweisungen der Knoten zur Richtlinie aufgehoben werden, finden Sie unter Zuweisung von Knoten zu Richtlinien aufheben (siehe Seite 67).

So löschen Sie Richtlinien

1. Melden Sie sich beim Virtual Standby-Server an und öffnen Sie Virtual Standby.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "VCM-Richtlinien".

   Das Fenster "Richtlinien" wird geöffnet.

2. Klicken Sie in der Liste "Richtlinien" auf die Richtlinie, die Sie löschen möchten.

3. Klicken Sie in der Symbolleiste "Richtlinien" auf "Löschen".

   Eine Bestätigungsmeldung des Löschvorgangs wird angezeigt.

4. Klicken Sie auf "Ja", um die Richtlinie zu löschen.

   Hinweis: Wenn Sie eine Richtlinie versehentlich löschen, müssen Sie die Richtlinie erneut erstellen. Wenn Sie die Richtlinie nicht löschen möchten, klicken Sie auf "Nein".

Die Richtlinie wird gelöscht.

Konfigurationsaufgaben der Anwendung

Virtual Standby ermöglicht es Ihnen, E-Mail-Warnmeldungseinstellungen festzulegen, und Sie können außerdem angeben, wie Ihre Virtual Standby-Installation aktualisiert werden soll.

Dieser Abschnitt enthält folgende Themen:

Konfigurieren der E-Mail-Einstellungen (siehe Seite 69)
Konfigurieren automatischer Updates (siehe Seite 70)
Konfigurieren von Voreinstellungen für Social Networking (siehe Seite 73)
Ändern des Administratorkontos (siehe Seite 74)

Konfigurieren der E-Mail-Einstellungen

Sie können die E-Mail-Einstellungen für die Verwendung mit Ihrer Anwendung konfigurieren, um gemäß der Bedingungen, die Sie angeben, automatische Warnmeldungen zu versenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Konfiguration" um die Ansicht "Konfiguration" zu öffnen.

2. Klicken Sie im Feld "Konfiguration" auf "E-Mail-Konfiguration", um die Optionen der E-Mail-Konfiguration anzuzeigen.

3. Füllen Sie die folgenden Felder aus:

   - **Dienst**: Geben Sie im Drop-down-Feld den Typ des E-Mail-Dienstes. (Google Mail, Yahoo Mail, Live Mail oder andere)
   - **E-Mail-Server**: Geben Sie den Hostnamen des SMTP-Servers an, den CA ARCserve Central Applications verwenden soll, um E-Mails zu senden.
   - **Erfordert Authentifizierung**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server, Authentifizierung benötigt. Der Kontoname und das Kennwort müssen angegeben werden.
   - **Betreff**: Geben Sie einen standardmäßigen E-Mail-Betreff an.
   - **Von**: Geben Sie die E-Mail-Adresse an, von der die E-Mail geschickt wird.
   - **Empfänger**: Geben Sie eine oder mehrere durch Semikolon (;) getrennte E-Mail-Adressen an, an die die E-Mail geschickt wird.

- **SSL verwenden**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server eine sichere Verbindung (SSL) erfordert.
- **STARTTLS senden**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server einen STARTTLS-Befehl erfordert.
- **HTML-Format verwenden**: Ermöglicht es Ihnen, die E-Mails in HTML-Format zu senden. (Standardmäßig ausgewählt)
- **Proxy-Einstellungen aktivieren**: Wählen Sie diese Option aus, wenn ein Proxy-Server vorhanden ist, und geben Sie anschließend die Proxy-Server-Einstellungen an.

4. Klicken Sie auf "Test-E-Mail", um zu sicherzustellen, dass die E-Mail-Konfigurationseinstellungen richtig sind.
5. Klicken Sie auf "Speichern".

   Hinweis: Sie können auf "Zurücksetzen" klicken, um zu den zuvor gespeicherten Werten zurückzukehren.

Die E-Mail-Konfiguration wird angewendet.

Konfigurieren automatischer Updates

Mit CA ARCserve Central Virtual Standby können Sie angeben, wann nach Produktaktualisierungen gesucht werden soll und wie oft Ihre Virtual Standby-Installation aktualisiert werden soll.

So konfigurieren Sie automatische Updates

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie in der Navigationsleiste auf "Konfiguration", um die Ansicht "Konfiguration" zu öffnen.
3. Klicken Sie im Konfigurationsbereich auf "Konfiguration aktualisieren".

   Die Optionen für die Aktualisierung der Konfiguration werden angezeigt.

4. Wählen Sie einen Download-Server aus.

   - **CA-Server:** Klicken Sie für folgende Optionen auf "Proxy-Einstellungen":

     - **Proxy-Einstellungen des Browsers verwenden:** Lässt Sie die Anmeldeinformationen verwenden, die für die Proxy-Einstellungen des Browsers vorbereitet wurden.

       Hinweis: Die Option "Proxy-Einstellungen des Browsers verwenden" wirkt sich auf Internet Explorer und Chrome aus.

     - **Proxy-Einstellungen konfigurieren:** Legen Sie die IP-Adresse oder den Hostnamen des Proxy-Servers und die Portnummer fest. Wenn der Server, den Sie angegeben haben, Authentifizierung erfordert, klicken Sie auf die Option "Proxy-Server erfordert Authentifizierung" und geben Sie die Anmeldeinformationen ein.

       Klicken Sie auf "OK", um zur Konfiguration der Aktualisierung zurückzukehren.

   - **Staging-Server**: Wenn Sie diese Option auswählen, klicken Sie auf "Server hinzufügen", um einen Staging-Server zur Liste hinzuzufügen. Geben Sie seinen Hostnamen und die Portnummer ein, und klicken Sie auf "OK".

     Wenn Sie mehrere Staging-Server angeben, versucht die Anwendung, den ersten der aufgelisteten Server zu verwenden. Wenn die Verbindung erfolgreich ist, werden die verbleibenden aufgelisteten Server nicht für das Staging verwendet.

5. (Optional) Klicken Sie auf "Verbindung testen", um die Serververbindung zu überprüfen und warten Sie, bis der Test abgeschlossen ist.

6. (Optional) Klicken Sie auf die Option "Automatisch nach Aktualisierungen suchen" und legen Sie den Tag und die Zeit fest. Sie können einen täglichen oder wöchentlichen Ablaufplan angeben.

Klicken Sie auf "Speichern", um die Konfiguration der Aktualisierung anzuwenden.

Proxy-Einstellungen konfigurieren

CA ARCserve Central Applications lässt Sie einen Proxy-Server zur Kommunikation mit CA Support festlegen, um nach verfügbaren Aktualisierungen zu überprüfen und sie herunterzuladen. Um diese Möglichkeit zu aktivieren, geben Sie den Proxy-Server an, mit dem Sie anstelle des CA ARCserve Central Applications-Servers kommunizieren wollen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

2. Klicken Sie auf "Konfiguration aktualisieren".

   Die Optionen für die Aktualisierung der Konfiguration werden angezeigt.

3. Klicken Sie auf Proxy-Einstellungen.

   Das Dialogfeld "Proxy-Einstellungen" wird geöffnet.

4. Aktivieren Sie eine der folgenden Optionen:

   - **Proxy-Einstellungen des Browsers verwenden:** Lässt die Anwendung die gleichen Proxy-Einstellungen erkennen und verwenden, die auf den Browser angewendet werden, um für den Erhalt von Aktualisierungsinformationen mit dem CA Technologies-Server zu kommunizieren.

     Hinweis: Dieses Verhalten bezieht sich nur auf Internet Explorer- und Chrome-Browser.

   - **Proxy-Einstellungen konfigurieren:** Lässt Sie einen alternativen Server festlegen, den die Anwendung verwenden wird, um mit CA Support zu kommunizieren und nach Aktualisierungen zu prüfen. Der alternative Server (Proxy) hilft dabei, mehr Sicherheit, erhöhte Leistung und Verwaltungskontrolle zu bieten.

Füllen Sie die folgenden Felder aus:

- **Proxy-Server:** Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers an.
- **Port:** Geben Sie die Portnummer an, die der Proxy-Server verwenden wird, um mit der CA Support-Website zu kommunizieren.
- **(Optional) Proxy-Server erfordert Authentifizierung:** Falls die Anmeldeinformationen für den Proxy-Server nicht die gleichen sind wie die Anmeldeinformationen für den CA ARCserve Central Applications-Server, aktivieren Sie das Kontrollkästchen neben "Proxy-Server erfordert Authentifizierung" und legen Sie den Benutzernamen und das Kennwort fest, die erforderlich sind, um sich beim Proxy-Server anzumelden.

  Hinweis: Verwenden Sie das folgende Format, um den Benutzernamen anzugeben: <Domänenname>\<Benutzername>.

Klicken Sie auf "OK".

Die Proxy-Einstellungen sind konfiguriert.

Konfigurieren von Voreinstellungen für Social Networking

CA ARCserve Central Applications lässt Sie die Social Networking-Tools verwalten, die Ihnen dabei helfen, die Anwendung zu verwalten. Sie können Nachrichten-Feeds generieren, Verknüpfungen zu beliebten Social Networking-Websites angeben und Videoquellen-Websites auswählen.

So konfigurieren Sie Voreinstellungen für Social Networking

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Konfiguration".

   Der Bildschirm "Konfiguration" wird angezeigt.

2. Klicken Sie im Konfigurationsbereich auf "Konfiguration der Voreinstellungen".

   Die Optionen der Voreinstellungen werden angezeigt.

3. Legen Sie die benötigten Optionen fest.

   - **Nachrichten-Feed:** Ermöglicht es, dass die Anwendung RSS-Feeds über mit CA ARCserve Central Applications und CA ARCserve D2D in Zusammenhang stehenden Nachrichten und Produktinformationen (aus dem Expertenforum) anzeigt. Die Feeds werden auf der Startseite angezeigt.
   - **Social Networking:** Ermöglicht es, dass die Anwendung auf der Startseite Zugriffssymbole auf Twitter und Facebook für mit CA ARCserve Central Applications und CA ARCserve D2D im Zusammenhang stehende Social Networking-Websites anzeigt.
   - **Videos:** Ermöglicht es Ihnen, den Videotyp auszuwählen, um Ihre Produkte von CA ARCserve Central Applications und CA ARCserve D2D anzuzeigen. ("YouTube-Videos verwenden" ist das Standardvideo.)

   Klicken Sie auf "Speichern".

   Die Social Networking-Optionen werden angewendet.

4. Klicken Sie in der Navigationsleiste auf "Start".

   Die Startseite wird geöffnet.

5. Aktualisieren Sie Ihren Browser.

   Die Social Networking-Optionen werden angewendet.

Ändern des Administratorkontos

CA ARCserve Central Applications lässt Sie den Benutzernamen, das Kennwort, oder beides für das Administratorkonto ändern, nachdem Sie die Anwendung installiert haben. Dieses Administratorkonto wird im Anmeldefenster nur für den standardmäßigen Anzeigebenutzernamen verwendet.

Hinweis: Der angegebene Benutzername muss ein Windows-Administratorkonto oder ein Konto sein, das Windows-Administratorrechte hat.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

2. Klicken Sie auf "Administratorkonto".

3. Die Administratorkontoeinstellungen werden angezeigt.
4. Aktualisieren Sie folgende Felder je nach Bedarf:
   - Benutzername
   - Kennwort

   Klicken Sie auf "Speichern".

Das Administratorkonto wurde geändert.

Anzeigen von Protokollen

Das Anzeigeprotokoll enthält umfassende Informationen zu den Vorgängen, die von Ihrer Anwendung ausgeführt werden. Das Protokoll liefert einen Audit-Pfad für jeden ausgeführten Job (an erster Stelle werden die letzten Aktivitäten aufgelistet) und kann bei der Behebung von Fehlern hilfreich sein.

So zeigen Protokolle an

1. Klicken Sie auf der Startseite in der Navigationsleiste auf "Protokolle anzeigen".

   Das Fenster "Protokolle anzeigen" wird angezeigt.

2. Geben Sie in den Drop-down-Listen die Protokollinformationen an, die Sie anzeigen möchten.

   - **Schweregrad:** Lässt Sie den Schweregrad des Protokolls angeben, das Sie anzeigen möchten. Sie können folgende Schweregradoptionen angeben:
     - **Alle:** Zeigt alle Protokolle unabhängig vom Schweregrad an.
     - **Informationen:** Zeigt nur Protokolle an, die allgemeine Informationen beschreiben.
     - **Fehler:** Zeigt nur Protokolle an, die schwerwiegende Fehler beschreiben, die aufgetreten sind.
     - **Warnungen:** Zeigt nur Protokolle an, die aufgetretene Warnungen beschreiben.
     - **Fehler und Warnungen:** Zeigt nur schwerwiegende Fehler und Warnungen an, die aufgetreten sind.
   - **Module:** Lässt Sie das Modul festlegen, für das Sie Protokolle anzeigen möchten. Sie können folgende Moduloptionen angeben:
     - **Alle:** Zeigt Protokolle zu alle Anwendungskomponenten an.
     - **Allgemein:** Zeigt Protokolle zu allgemeinen Prozessen an.
     - **Knoten aus Datei importieren:** Zeigt nur Protokolle zum Importvorgang von CA ARCserve D2D-Knoten in die Anwendung aus einer Datei an.
     - **Richtlinienverwaltung:** Zeigt nur Protokolle zur Verwaltung von Richtlinien an.
     - **Aktualisierungen:** Zeigt nur Protokolle zur Aktualisierung der Anwendung an.
   - **Knotenname:** Zeigt nur Protokolle für bestimmte Knoten an.

     Hinweis: Dieses Feld unterstützt den Platzhalter '*' und '?'. Geben Sie zum Beispiel 'lod*' ein, um alle Aktivitätsprotokolle für den Computernamen zurückzugeben, der mit 'lod' anfängt.

Hinweis: Die Optionen "Schweregrad", "Module" und "Knotennamen" können zusammen angewendet werden. Sie können beispielsweise Fehler (Schweregrad) anzeigen, die sich auf Aktualisierungen (Module) für Knoten X (Knotenname) beziehen.

Klicken Sie auf "Aktualisieren".

Die Protokollanzeige basiert auf den festgelegten Anzeigeoptionen.

Hinweis: Die angezeigte Zeit basiert auf der Zeitzone des Datenbankservers Ihrer Anwendung.

Links zur Navigationsleiste hinzufügen

Jedes des CA ARCserve Central Applications verfügt in der Navigationsleiste über den Link "Neue Registerkarte hinzufügen". Verwenden Sie diese Funktion, um in der Navigationsleiste Einträge für zusätzliche webbasierte Anwendungen hinzuzufügen, die Sie verwalten möchten. Für jede installierte Anwendung wird automatisch eine neue Verknüpfung zur Navigationsleiste hinzugefügt. Wenn Sie beispielsweise CA ARCserve Central Reporting und CA ARCserve Central Virtual Standby auf "Computer A" installiert haben und CA ARCserve Central Reporting starten, wird CA ARCserve Central Virtual Standby automatisch zur Navigationsleiste hinzugefügt.

Hinweis: Die neu installierten Anwendungen werden nur entdeckt, wenn sich auf demselben Computer eine andere CA ARCserve Central Applications-Anwendung befindet.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste der Anwendung auf den Link "Neue Registerkarte hinzufügen".
2. Geben Sie den Namen und die URL der Anwendung oder Website an, die Sie hinzufügen wollen. Zum Beispiel, www.google.com.

   Geben Sie optional den Speicherort eines Symbols an.
3. Klicken Sie auf "OK".

   Die neue Registerkarte wird dem unteren Ende der Navigationsleiste hinzugefügt.

Beachten Sie Folgendes:

- Die CA Support-Verknüpfung wird Ihnen standardmäßig zur Verfügung gestellt.

  Sie können die neue Registerkarte entfernen, indem Sie sie markieren und auf "Entfernen" klicken.

Startseite von Virtual Standby

Die Registerkarte "Virtual Standby" auf dem Überwachungsserver ermöglicht es Ihnen, Informationen zu allen von Ihnen geschützten CA ARCserve D2D-Servern anzuzeigen. Auf der Registerkarte "Virtual Standby" auf Quellservern können Sie hingegen nur Informationen zu dem spezifischen Quellserver anzeigen, bei dem Sie sich anmelden.

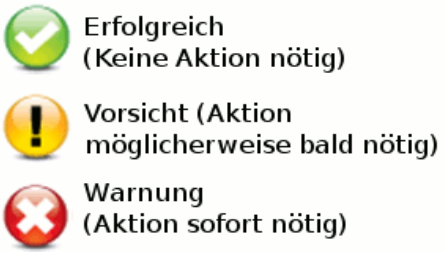
Dieser Abschnitt enthält folgende Themen:

So verwenden Sie den Bildschirm "Übersicht über Virtual Standby" (siehe Seite 78)
So verwenden Sie die Serverliste (siehe Seite 79)
Anzeigen von "Zusammenfassende Informationen" zum neuesten Virtual Standby-Job (siehe Seite 80)
Überwachen des Status von virtuellen Konvertierungsjobs (siehe Seite 81)
Anzeigen der Virtual Standby-Einstellungen für Quellserver (siehe Seite 82)
Anzeigen der Liste der Wiederherstellungspunkt-Snapshots (siehe Seite 83)

So verwenden Sie den Bildschirm "Übersicht über Virtual Standby"

Im Fenster "Übersicht über Virtual Standby" finden Sie Symbole zur schnellen, visuellen Anzeige des aktuellen Status sowie eine Anleitung für mögliche akut erforderliche Aktionen.

Folgende Symbole werden auf der Startseite angezeigt:



Das Fenster "Übersicht über Virtual Standby" zeigt folgende Informationen an:

- **Serverliste:** Zeigt eine Liste von Quellservern an, die dieser Überwachungsserver schützt. Die Liste sortiert Server nach ihrem aktuellen Status. Beispielsweise "Alle", "Aktion erforderlich", "Server wird ausgeführt" usw.

  Hinweis: Die Serverliste wird nur angezeigt, wenn Sie auf dem Überwachungsserver angemeldet sind. Weitere Informationen finden Sie unter So verwenden Sie die Serverliste (siehe Seite 79).

- **Übersicht über Virtual Standby**: Zeigt Übersichtsinformationen für den ausgewählten Quellserver an. Weitere Informationen finden Sie unter Überwachen des Status virtueller Konvertierungsjobs (siehe Seite 81).

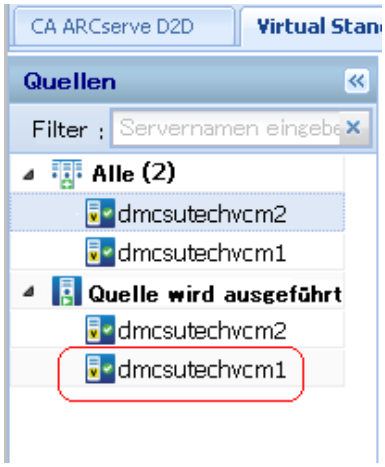
- **Virtual Standby-Einstellungen:** Zeigt Übersichtsinformationen über die Einstellungen der virtuellen Konvertierung für den ausgewählten Quellserver an. Weitere Informationen finden Sie unter Anzeigen von Virtual Standby-Einstellungen für Quellserver (siehe Seite 82).
- **Wiederherstellungspunkt-Snapshots:** Zeigt eine Liste von Wiederherstellungspunkt-Snapshots an, die für den ausgewählten Quellserver verfügbar sind. Weitere Informationen finden Sie unter Anzeigen der Liste von Wiederherstellungspunkt-Snapshots (siehe Seite 83).
- **Aufgaben:** Zeigt eine Liste von Aufgaben an, die Sie für den ausgewählten Quellserver ausführen können. Weitere Informationen finden Sie unter Überwachungsaufgaben von Virtual Standby (siehe Seite 83).
- **Zugriff auf Support und Community:** Stellt einen Mechanismus zur Verfügung, mit dem Sie verschiedene Support-bezogene Funktionen initiieren können.

  Hinweis: Weitere Informationen über den Zugriff auf Support und Community finden Sie in der CA ARCserve D2D-Dokumentation.

So verwenden Sie die Serverliste

Die Serverliste im Fenster "Übersicht über Virtual Standby" zeigt eine Liste von Quellservern an, die von einem Überwachungsserver geschützt werden. Die Liste sortiert Server nach ihrem aktuellen Status. Beispielsweise "Alle", "Aktion erforderlich", "Quelle wird ausgeführt" usw.

Um Verwaltungsaufgaben auszuführen oder Informationen über einen CA ARCserve D2D-Knoten anzuzeigen, klicken Sie auf die Registerkarte "Virtual Standby", und klicken Sie anschließend, wie im folgenden Fenster dargestellt, auf den Server:



Anzeigen von "Zusammenfassende Informationen" zum neuesten Virtual Standby-Job

Das Fenster "Knoten" ermöglicht es Ihnen, die zusammenfassenden Informationen über den letzten Virtual Standby-Job (Konvertierung) für einen Knoten anzuzeigen. Sie können Informationen über Virtual Standby-Jobs anzeigen, die mit oder ohne Erfolg abgeschlossen wurden.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Virtual Standby-Server an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Bewegen Sie in der Spalte "Status" Ihren Mauszeiger über eines der folgenden angezeigten Symbole:

   Erfolgreich

   Warnung

   Fehler/Fehlgeschlagen

   Das Feld "Knotenstatusübersicht" wird angezeigt und liefert Ihnen die folgenden Ergebnisse für den letzten erfolgreichen Virtual Standby-Job:

   Letzter Virtual Standby-Job

   Das Datum und die Uhrzeit des letzten Virtual Standby-Jobs, der erfolgreich oder erfolglos abgeschlossen hat.

   Wiederherstellungspunkt-Snapshots

   Zeigt die Anzahl von Wiederherstellungspunkten an, die ab dem letzten Virtual Standby für den Knoten konvertiert werden.

   Zielstatus

   Zeigt den verfügbaren freien Festplattenspeicherplatz auf dem Virtual Standby-Ziel an. Das Ziel kann aus Folgendem bestehen:

   - Ein ESX Server-Datenspeicher, der verwendet wird, um in ein ESX Server-System zu konvertieren.
   - Schaffen Sie Speicherplatz auf dem Volume, auf dem ein Hyper-V-Server die Wiederherstellungspunkt-Snapshots speichert.

3. Bewegen Sie Ihren Mauszeiger vom Symbol "Status" weg, um das Feld "Knotenstatusübersicht" zu schließen.
4. Sie können weitere Informationen über den letzten erfolgreichen oder erfolglosen Virtual Standby-Job in den folgenden Feldern anzeigen:

   Ergebnis der letzten Konvertierung

   Ergebnisse des letzten Virtual Standby-Jobs, der mit oder ohne Erfolg abgeschlossen wurde. Zum Beispiel "Abgeschlossen", "Abgebrochen" oder "Fehlgeschlagen".

   Zeitpunkt der letzten Konvertierung

   Das Datum und die Uhrzeit des letzten mit oder ohne Erfolg abgeschlossenen Virtual Standby-Jobs.

Überwachen des Status von virtuellen Konvertierungsjobs

Virtual Standby lässt Sie den Status von in Betrieb befindlichen virtuellen Konvertierungsjobs überwachen. Außerdem können Sie mithilfe von Virtual Standby Übersichtsinformationen über die virtuellen Konvertierungsdaten und die virtuellen Rechner anzeigen, die Ihre CA ARCserve D2D-Quellserver schützen.

So überwachen Sie den Status von virtuellen Konvertierungsjobs

1. Öffnen Sie "Virtual Standby", und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.
2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.
3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   CA ARCserve D2D wird geöffnet.

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

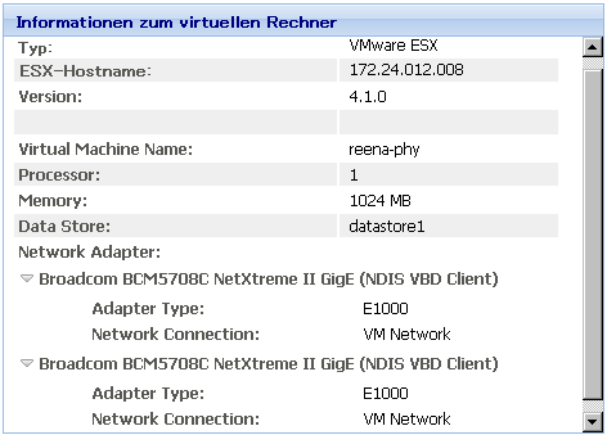
4. Klicken Sie auf die Registerkarte "Virtual Standby".

   (Optional) Wenn der CA ARCserve D2D-Server ein Überwachungsserver ist, klicken Sie auf die Serverliste, blenden Sie "Alle", "Quelle wird ausgeführt" oder "Aktion erforderlich" ein, und klicken Sie auf den Server, den Sie überwachen möchten.

   Virtual Standby zeigt Informationen über sich in Betrieb befindliche virtuelle Konvertierungsjobs und Übersichtsinformationen über virtuelle Konvertierungsjobs und den virtuellen Computer an, der den Server schützt.

Anzeigen der Virtual Standby-Einstellungen für Quellserver

Das Fenster "Übersicht über Virtual Standby" zeigt Informationen zu den virtuellen Rechnern an, die den Quellserver schützen.

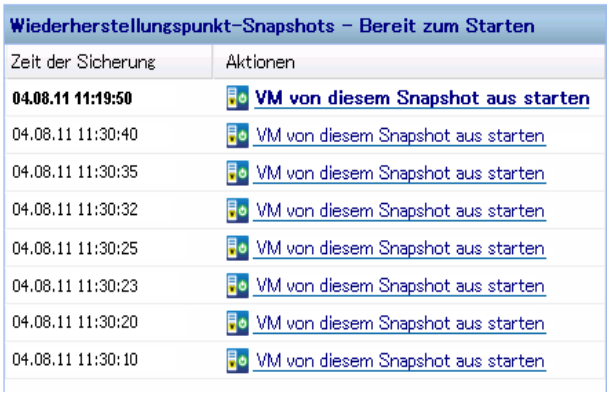


Anzeigen der Liste der Wiederherstellungspunkt-Snapshots

Das Fenster "Virtual Standby" zeigt eine Liste der neuesten Wiederherstellungspunkt-Snapshots an.

Das Listenfeld zeigt das Datum und die Uhrzeit an, zu der die Sicherung des CA ARCserve D2D-Servers abgeschlossen wurde.

Sie virtuelle Rechner in der Liste der Wiederherstellungspunkt-Snapshots einschalten. Weitere Informationen finden Sie unter Inbetriebnahme von Wiederherstellungspunkt-Snapshots (siehe Seite 90).



Hinweis: Wenn das Virtual Standby-Ziel ein VMware ESX-Server ist, ist die Höchstanzahl von Wiederherstellungspunkt-Snapshots, die angezeigt werden, 29. Wenn das Virtual Standby-Ziel ein Microsoft Hyper-V-Server ist, ist die Höchstanzahl von Wiederherstellungspunkt-Snapshots, die angezeigt werden, 24.

CA ARCserve Central Virtual Standby-Überwachungs-Aufgaben

Virtual Standby lässt Sie folgende Überwachungsaufgaben ausführen:

- Heartbeat-Signale aussetzen und wieder aufnehmen (siehe Seite 84).
- Virtual Standby-Jobs aussetzen und wieder aufnehmen (siehe Seite 87).
- Anzeigen von Aktivitätsprotokolldaten über virtuelle Konvertierungen und Wiederherstellungspunkt-Snapshots (siehe Seite 94).
- Inbetriebnahme von Wiederherstellungspunkt-Snapshots (siehe Seite 90).

Unterbrechen und Wiederaufnehmen von Heartbeat-Signalen des Virtual Standby-Servers

Virtual Standby lässt Sie vom Überwachungsserver erkannte Heartbeat-Signale aussetzen und wieder aufnehmen. Heartbeat ist der Prozess, bei dem die Quellserver und Überwachungsserver über den Zustand des Quellservers kommunizieren. Wenn der Überwachungsserver nach Ablauf eines festgelegten Zeitraums kein Heartbeat-Signal erkennt, stellt Virtual Standby den virtuellen Rechner bereit, damit dieser als Quellknoten fungiert.

Beispiele: Wann sollen Heartbeat-Signale ausgesetzt und wann fortgesetzt werden

Die folgenden Beispiele beschreiben, wann Sie Heartbeat-Signale aussetzen und wann Sie sie fortsetzen sollten:

- Setzen Sie das Heartbeat-Signal aus, wenn Sie einen Knoten (Quellserver) für Wartungszwecke offline setzen wollen.
- Setzen Sie das Heartbeat-Signal fort, nachdem die Wartungsaufgaben abgeschlossen wurden und der Knoten (Quellserver) wieder online ist.

Beachten Sie Folgendes:

- Sie können Heartbeat-Signale unterbrechen und sie auf Gruppenebene oder auf der individuellen Knotenebene wiederaufnehmen.
- Sie können Heartbeat-Signale für einen oder mehrere Knoten in einem Schritt unterbrechen und wiederaufnehmen.
- CA ARCserve Central Virtual Standby setzt keine Wiederherstellungspunkt-Snapshots in Betrieb, solange sich das Heartbeat-Signal in einem angehaltenen Status befindet.
- Wenn Sie für die CA ARCserve D2D-Installationen ein Upgrade auf Quellknoten durchführen, setzt CA ARCserve Central Virtual Standby das Heartbeat-Signal für die Knoten aus. Um sicherzustellen, dass Überwachungsserver die Knoten, für die ein Upgrade durchgeführt wurde, überwachen, nehmen Sie das Heartbeat-Signal für die Knoten wieder auf, nachdem die Upgrades abgeschlossen wurden.

Hinweis: Optional können Sie Heartbeat-Signale über das Fenster "Übersicht über Virtual Standby" auf dem Knoten unterbrechen oder wiederaufnehmen. Weitere Informationen zum Unterbrechen und Wiederaufnehmen von Heartbeat-Signalen von Knoten (siehe Seite 86).

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Virtual Standby-Server an.

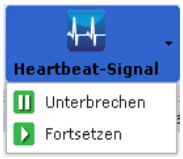
   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Führen Sie eine der folgenden Aktionen aus, um die Knoten festzulegen, die Sie unterbrechen oder wiederaufnehmen wollen:

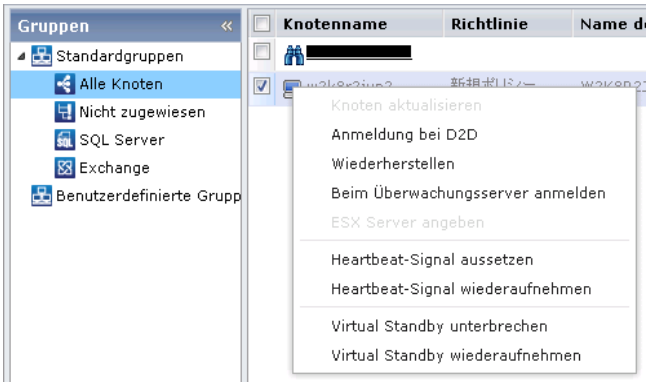
   - **Knotenebene:** Klicken Sie auf die Gruppe, die die Knoten enthält, die Sie unterbrechen oder wiederaufnehmen wollen, und aktivieren Sie die Kontrollkästchen neben den Knoten, die Sie unterbrechen oder wiederaufnehmen wollen.
   - **Gruppenebene:** Klicken Sie auf die Gruppe, die die Knoten enthält, die Sie unterbrechen oder wiederaufnehmen wollen.

3. Führen Sie eine der folgenden Aktionen aus, um das Heartbeat-Signal zu unterbrechen oder wiederaufzunehmen:

   - Klicken Sie in der Symbolleiste auf "Heartbeat-Signal" und klicken Sie auf im Pop-up-Menü auf "Unterbrechen" oder "Wiederaufnehmen", wie im folgenden Fenster dargestellt:

   - Klicken Sie mit der rechten Maustaste auf die ausgewählte Gruppe oder klicken Sie mit der rechten Maustaste auf die Knoten und klicken Sie im Pop-up-Menü auf "Heartbeat-Signal unterbrechen" oder "Heartbeat-Signal wiederaufnehmen", wie im folgenden Fenster dargestellt:

Unterbrechen und Wiederaufnehmen von Heartbeat-Signalen von den Knoten aus

Virtual Standby lässt Sie vom Überwachungsserver erkannte Heartbeat-Signale aussetzen und wieder aufnehmen. Heartbeat ist der Prozess, bei dem die Quellserver und Überwachungsserver über den Zustand des Quellservers kommunizieren. Wenn der Überwachungsserver nach Ablauf eines festgelegten Zeitraums kein Heartbeat-Signal erkennt, stellt Virtual Standby den virtuellen Rechner bereit, damit dieser als Quellknoten fungiert.

Beispiele: Wann sollen Heartbeat-Signale ausgesetzt und wann fortgesetzt werden

Die folgenden Beispiele beschreiben, wann Sie Heartbeat-Signale aussetzen und wann Sie sie fortsetzen sollten:

- Setzen Sie das Heartbeat-Signal aus, wenn Sie einen Knoten (Quellserver) für Wartungszwecke offline setzen wollen.
- Setzen Sie das Heartbeat-Signal fort, nachdem die Wartungsaufgaben abgeschlossen wurden und der Knoten (Quellserver) wieder online ist.

Hinweis: Optional können Sie Heartbeat-Signale vom Fenster "Knoten" aus auf dem Virtual Standby-Server unterbrechen und wiederaufnehmen. Weitere Informationen zum Unterbrechen und Wiederaufnehmen von Heartbeat-Signalen vom Virtual Standby-Server aus (siehe Seite 84).

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Virtual Standby-Server an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, dessen Heartbeat-Signal Sie aussetzen oder wiederaufnehmen möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   CA ARCserve D2D wird geöffnet.

4. Klicken Sie auf die Registerkarte "Virtual Standby".

   Das Fenster "Übersicht über Virtual Standby" wird geöffnet.

5. (Optional) Wenn Sie auf einem Überwachungsserver angemeldet sind, blenden Sie in der Serverliste "Alle" oder "Server wird ausgeführt" ein, und klicken auf den Knoten, dessen Heartbeat-Signal Sie aussetzen oder wieder aufnehmen möchten.

   Hinweis: Wenn die Heartbeat-Signale ausgeführt werden, wird in der Aufgabenliste der virtuellen Konvertierung "Heartbeat-Signal aussetzen" angezeigt. Wenn die Heartbeat-Signale ausgeführt werden, wird in der Aufgabenliste der virtuellen Konvertierung "Heartbeat-Signal wieder aufnehmen" angezeigt.

6. Wählen Sie eine der folgenden Vorgehensweisen:

   - Wenn die Heartbeat-Signale ausgeführt werden, klicken Sie auf "Heartbeat-Signal aussetzen", um die Heartbeat-Signale anzuhalten.

     Beispiel: Sie möchten den Server offline setzen, um Verwaltungsaufgaben auszuführen.

   - Wenn das Heartbeat-Signal nicht ausgeführt wird (angehalten), klicken Sie auf "Heartbeat-Signal wieder aufnehmen", um das Heartbeat-Signal wieder aufzunehmen.

     Beispiel: Die Verwaltungsaufgaben sind abgeschlossen, und Sie möchten den Server online setzen.

Das Heartbeat-Signal wird ausgesetzt oder wieder aufgenommen.

Unterbrechen und Wiederaufnehmen von Virtual Standby-Jobs vom Virtual Standby-Server aus

Virtuelle Konvertierung ist der Prozess, bei dem Virtual Standby CA ARCserve D2D-Wiederherstellungspunkte von Quellknoten in Datendateien virtueller Rechner konvertiert, die als Wiederherstellungspunkt-Snapshots bezeichnet werden. Wenn ein Quellknoten fehlschlägt, verwendet Virtual Standby die Wiederherstellungspunkt-Snapshots, um einen virtuellen Rechner für den Quellknoten in Betrieb zu nehmen.

Die Best Practice besteht darin, zuzulassen, dass der virtuelle Konvertierungsprozess kontinuierlich in Betrieb ist. Wenn Sie den virtuellen Konvertierungsprozess jedoch zeitweise unterbrechen wollen, können Sie dies über den Virtual Standby-Server tun. Nachdem Sie die Probleme auf dem Quellknoten behoben haben, können Sie den virtuellen Konvertierungsprozess wieder aufnehmen.

Hinweis: Optional können Sie Virtual Standby-Jobs direkt von den Knoten aus unterbrechen und wiederaufnehmen. Weitere Informationen finden Sie unter Aussetzen und Wiederaufnehmen von Virtual Standby-Jobs von Knoten aus (siehe Seite 88).

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Virtual Standby-Server an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Führen Sie eine der folgenden Aktionen aus, um die Knoten festzulegen, auf denen Sie Virtual Standby-Jobs unterbrechen oder wiederaufnehmen wollen:

   - **Knotenebene:** Klicken Sie auf die Gruppe, die die Knoten enthält, die Sie unterbrechen oder wiederaufnehmen wollen, und aktivieren Sie die Kontrollkästchen neben den Knoten, die Sie unterbrechen oder wiederaufnehmen wollen.
   - **Gruppenebene:** Klicken Sie auf die Gruppe, die die Knoten enthält, die Sie unterbrechen oder wiederaufnehmen wollen.

3. Führen Sie eine der folgenden Aktionen aus, um die Virtual Standby-Jobs zu unterbrechen oder wiederaufzunehmen:

   - Klicken Sie in der Symbolleiste auf Virtual Standby und klicken Sie im Pop-up-Menü auf "Unterbrechen" oder "Wiederaufnehmen".
   - Klicken Sie auf die ausgewählte Gruppe oder klicken Sie auf die Knoten und klicken Sie im Pop-up-Menü auf "Virtual Standby unterbrechen" oder "Virtual Standby wiederaufnehmen".

Unterbrechen und Wiederaufnehmen von Virtual Standby-Jobs von den Knoten aus

Virtuelle Konvertierung ist der Prozess, bei dem Virtual Standby CA ARCserve D2D-Wiederherstellungspunkte von Quellknoten in Datendateien virtueller Rechner konvertiert, die als Wiederherstellungspunkt-Snapshots bezeichnet werden. Wenn ein Quellknoten fehlschlägt, verwendet Virtual Standby die Wiederherstellungspunkt-Snapshots, um einen virtuellen Rechner für den Quellknoten in Betrieb zu nehmen.

Die Best Practice besteht darin, zuzulassen, dass der virtuelle Konvertierungsprozess kontinuierlich in Betrieb ist. Wenn Sie den virtuellen Konvertierungsprozess jedoch zeitweise unterbrechen wollen, können Sie dies über den Virtual Standby-Server tun. Nachdem Sie die Probleme auf dem Quellknoten behoben haben, können Sie den virtuellen Konvertierungsprozess wieder aufnehmen.

Hinweis: Optional können Sie Virtual Standby-Jobs vom Virtual Standby-Server aus unterbrechen und wiederaufnehmen. Weitere Informationen finden Sie unter Aussetzen und Wiederaufnehmen von Virtual Standby-Jobs vom Virtual Standby-Server aus (siehe Seite 87).

Gehen Sie wie folgt vor:

1. Öffnen Sie "Virtual Standby", und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, dessen Virtual Standby-Jobs Sie aussetzen oder wiederaufnehmen möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   CA ARCserve D2D wird geöffnet.

4. Klicken Sie auf die Registerkarte "Virtual Standby".

   Das Fenster "Übersicht über Virtual Standby" wird geöffnet.

5. (Optional) Wenn Sie auf einem Überwachungsserver angemeldet sind, blenden Sie in der Serverliste "Alle" oder "Server wird ausgeführt" ein, und klicken auf den Knoten, dessen Virtual Standby-Job Sie aussetzen oder wieder aufnehmen möchten.

   Wenn der Virtual Standby-Job ausgeführt wird, wird in der Aufgabenliste von "Virtual Standby" "Virtual Standby unterbrechen" angezeigt. Wenn der Virtual Standby-Job nicht ausgeführt wird, wird in der Aufgabenliste von "Virtual Standby" "Virtual Standby wiederaufnehmen" angezeigt.

6. Wählen Sie eine der folgenden Vorgehensweisen:

   - Wenn der Virtual Standby-Job ausgeführt wird, klicken Sie auf "Virtual Standby unterbrechen", um den Job zeitweilig zu auszusetzen.
   - Wenn der Virtual Standby-Job nicht ausgeführt wird (angehalten), klicken Sie auf "Virtual Standby wiederaufnehmen", um den Job fortzusetzen.

Der Virtual Standby-Job wird ausgesetzt oder wieder aufgenommen.

Einschalten von virtuellen Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots

Virtual Standby kann so konfiguriert werden, dass Wiederherstellungspunkt-Snapshots automatisch in Betrieb genommen werden, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver entdeckt. Optional können Sie mit Virtual Standby Wiederherstellungspunkt-Snapshots manuell in Betrieb nehmen, falls ein Quellserver fehlschlägt, ein Notfall eintritt oder Sie einen Quellserver zur Wartung offline schalten wollen.

Hinweis: Die folgenden Schritte beschreiben, wie sie virtuelle Virtual Standby-Rechner manuell aus Wiederherstellungspunkt-Snapshots einschalten. Weitere Informationen darüber, wie Sie Wiederherstellungspunkt-Snapshots mit Virtual Standby automatisch einschalten können, finden Sie unter Erstellen von Richtlinien (siehe Seite 32).

Gehen Sie wie folgt vor:

1. Öffnen Sie "Virtual Standby" und klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.
2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.
3. Navigieren Sie zu dem Knoten, den Sie von einem Wiederherstellungs-Snapshot aus einschalten möchten, und klicken Sie auf den Knoten; klicken Sie dann auf "Standby-VM" in der Symbolleiste "Aktionen".

   Das Dialogfeld "Wiederherstellungspunkt-Snapshots" wird geöffnet.
4. Geben Sie im Wiederherstellungspunkt-Snapshot-Dialogfeld einen Datums-und Uhrzeitbereich an, um den Wiederherstellungspunkt-Snapshot zu finden, den Sie verwenden wollen.

   Klicken Sie auf "VM starten".

Der virtuelle Rechner wird unter Verwendung der im Wiederherstellungspunkt-Snapshot enthaltenen Daten eingeschaltet.

Hinweis: Nachdem der virtuelle Rechner eingeschaltet wurde, werden Sie möglicherweise aufgefordert, den Computer einmal oder mehrmals neu zu starten. Dieses Verhalten tritt auf, da auf dem virtuellen Rechner VMware Tools durch VMware und Hyper-V-Integrationsdienste durch Windows installiert werden.

Nachdem Sie virtuelle Virtual Standby-Rechner von Wiederherstellungspunkt-Snapshots eingeschaltet haben, müssen Sie möglicherweise folgende Aufgaben ausführen:

- Aktivieren Sie das Windows-Betriebssystem, das auf dem virtuellen Rechner ausgeführt wird.
- Starten Sie CA ARCserve D2D-Sicherungen auf dem virtuellen Rechner.

  Hinweis: Informationen über das Erstellen und Zuweisen von CA ARCserve D2D-Sicherungsrichtlinien mithilfe von CA ARCserve Central Protection Manager finden Sie im *CA ARCserve Central Protection Manager-Benutzerhandbuch.*
- Aktualisieren Sie CA ARCserve Central Virtual Standby mit dem Hostnamen, IP-Adresse und den Anmeldeinformationen für den virtuellen Rechner.
- Weisen Sie den Knoten einer Richtlinie zu.

  Hinweis: Diese Aufgabe ist nur erforderlich, wenn Sie Wiederherstellungspunkt-Snapshots für den eingeschalteten virtuellen Rechner erstellen möchten. Weitere Informationen finden Sie unter Zuweisen von Knoten zu einer Richtlinie (siehe Seite 39).

Einschalten von virtueller Virtual Standby-Rechner über den Hyper-V-Manager

Wenn Sie virtuelle Virtual Standby-Rechner manuell einschalten möchten, sollten Sie als Best Practice die virtuellen Rechner über das Fenster "Virtual Standby" auf dem CA ARCserve D2D-Server einschalten. Weitere Informationen finden Sie unter Einschalten von virtuellen Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots (siehe Seite 90). Wenn Sie virtuelle Virtual Standby-Rechner über den Hyper-V-Server starten möchten, können Sie dies allerdings mithilfe von Hyper-V-Manager tun.

Hinweis: Der Hyper-V-Manager ermöglicht Ihnen den Zugriff auf die Wiederherstellungspunkt-Snapshots, die CA ARCserve Central Virtual Standby erstellt hat, um den Knoten zu schützen. Sie sollten diese Snapshots nicht löschen. Wenn Sie die Snapshots löschen, wird die Beziehung zwischen den in den Snapshots enthaltenen Daten bei der nächsten Ausführung von Virtual Standby inkonsistent. Mit inkonsistenten Daten können Sie virtuelle Virtual Standby-Rechner nicht korrekt einschalten.

So schalten Sie virtuelle Virtual Standby-Rechner über den Hyper-V-Manager ein

1. Melden Sie sich beim Hyper-V-Server an, der die Knoten überwacht, die Sie schützen.
2. Starten Sie den Hyper-V-Manager durch folgende Schritte:

   Klicken Sie auf "Start", dann auf "Programme" und anschließend auf "Hyper-V-Manager.

   Hyper-V-Manager wird geöffnet.

3. Blenden Sie in der Verzeichnisstruktur des Hyper-V-Managers "Hyper-V-Manager" ein, und klicken Sie auf den Hyper-V-Server, der den virtuellen Rechner enthält, den Sie einschalten möchten.

   Die virtuellen Rechner, die mit dem angegebenen Hyper-V-Server verbunden sind, werden in der Liste "Virtuelle Computer" im Hauptfenster angezeigt.

4. Wählen Sie eine der folgenden Vorgehensweisen:

   - **Um den virtuellen Rechner unter Verwendung des neuesten Snapshot einzuschalten:** Klicken Sie in der Liste "Virtuelle Computer" mit der rechten Maustaste auf den virtuellen Rechner, den Sie einschalten möchten, und anschließend im Pop-up-Menü auf "Start".
   - **Um den virtuellen Rechner mithilfe eines älteren Snapshot einzuschalten:**

     a. Klicken Sie in der Liste "Virtuelle Computer" mit der rechten Maustaste auf den virtuellen Rechner, den Sie einschalten möchten.

        Die Snapshots, die mit dem virtuellen Rechner verbunden sind, werden in der Liste "Snapshots" angezeigt.

     b. Klicken Sie mit der rechten Maustaste auf den Snapshot, den Sie verwenden möchten, um den virtuellen Rechner einzuschalten, und klicken Sie im Pop-up-Menü auf "Anwenden".

        Der Dialogfeld "Snapshot anwenden" wird geöffnet.

     c. Klicken Sie auf "Übernehmen".

     d. Klicken Sie in der Liste "Virtuelle Computer" mit der rechten Maustaste auf den virtuellen Rechner, den Sie einschalten möchten, und anschließend im Pop-up-Menü auf "Start".

   Der virtuelle Virtual Standby-Rechner ist eingeschaltet.

Wenn nötig, können Sie die virtuellen Rechner sichern und Wiederherstellungspunkt-Snapshots erstellen, nachdem Sie den virtuellen Rechner eingeschaltet haben. Weitere Informationen finden Sie unter Auszuführende Aufgaben nach dem Einschalten von virtuellen Virtual Standby-Rechnern.

Einschalten von virtuellen Virtual Standby-Rechnern über VMware vSphere Client

Wenn Sie virtuelle Virtual Standby-Rechner manuell einschalten möchten, sollten Sie als Best Practice die virtuellen Rechner über das Fenster "Virtual Standby" auf dem CA ARCserve D2D-Server einschalten. Weitere Informationen finden Sie unter Einschalten von virtuellen Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots (siehe Seite 90). Wenn Sie die virtuellen Virtual Standby-Rechner über das ESX Server- oder vCenter Server-System starten möchten, können Sie dies allerdings über VMware vSphere Client tun.

Hinweis: Der VMware vSphere Client ermöglicht Ihnen den Zugriff auf die Wiederherstellungspunkt-Snapshots, die CA ARCserve Central Virtual Standby erstellt hat, um den Knoten zu schützen. Sie sollten diese Snapshots nicht löschen. Wenn Sie die Snapshots löschen, wird die Beziehung zwischen den in den Snapshots enthaltenen Daten bei der nächsten Ausführung von Virtual Standby inkonsistent. Mit inkonsistenten Daten können Sie virtuelle Virtual Standby-Rechner nicht korrekt einschalten.

So schalten Sie virtuelle Virtual Standby-Rechner über VMware vSphere Client ein

1. Öffnen Sie VMware vSphere Client, und melden Sie sich beim ESX Server- oder vCenter Server-System an, das die Knoten überwacht, die Sie schützen.

   Blenden Sie in der Verzeichnisstruktur das ESX Server-System oder vCenter Server-System ein, durchsuchen Sie es, und klicken Sie auf den virtuellen Rechner, den Sie einschalten möchten

2. Wählen Sie eine der folgenden Vorgehensweisen:

   - **Um den virtuellen Rechner unter Verwendung des neuesten Snapshot einzuschalten:** Klicken Sie auf die Registerkarte "Getting Started" und anschließend unten im Fenster auf "Power on the virtual machine" (Virtuellen Rechner einschalten).
   - **Um den virtuellen Rechner mithilfe eines älteren Snapshot einzuschalten:**

     a. Klicken Sie in der Symbolleiste auf die Schaltfläche "Snapshot Manager" .

     Das Dialogfeld "Snapshots for (Name des virtuellen Rechners) wird geöffnet, um eine Liste der Snapshots anzuzeigen, die für den virtuellen Rechner zur Verfügung stehen.

     b. Klicken Sie in der Snapshot-Liste auf den Snapshot, den Sie verwenden möchten, um den virtuellen Rechner einzuschalten, und anschließend auf "Go".

   Der virtuelle Virtual Standby-Rechner ist eingeschaltet.

Wenn nötig, können Sie die virtuellen Rechner sichern und Wiederherstellungspunkt-Snapshots erstellen, nachdem Sie den virtuellen Rechner eingeschaltet haben. Weitere Informationen finden Sie unter Auszuführende Aufgaben nach dem Einschalten von virtuellen Virtual Standby-Rechnern.

Anzeigen von Aktivitätsprotokolldaten über Jobs

Virtual Standby lässt Sie Informationen über das Aktivitätsprotokoll zu virtuellen Konvertierungsjobs anzeigen. Das Aktivitätsprotokoll enthält Datensätze virtueller Konvertierungsjobs für die CA ARCserve D2D-Quellserver, die Sie schützen.

Hinweis: Das Aktivitätsprotokoll (activity.log) wird im folgenden Verzeichnis auf dem Server gespeichert, in dem CA ARCserve D2D installiert ist:

```
C:\Programme\CA\ARCserve D2D\Protokolle
```

So zeigen Sie Aktivitätsprotokolldaten über Jobs an

1. Öffnen Sie "Virtual Standby", und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   CA ARCserve D2D wird geöffnet.

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

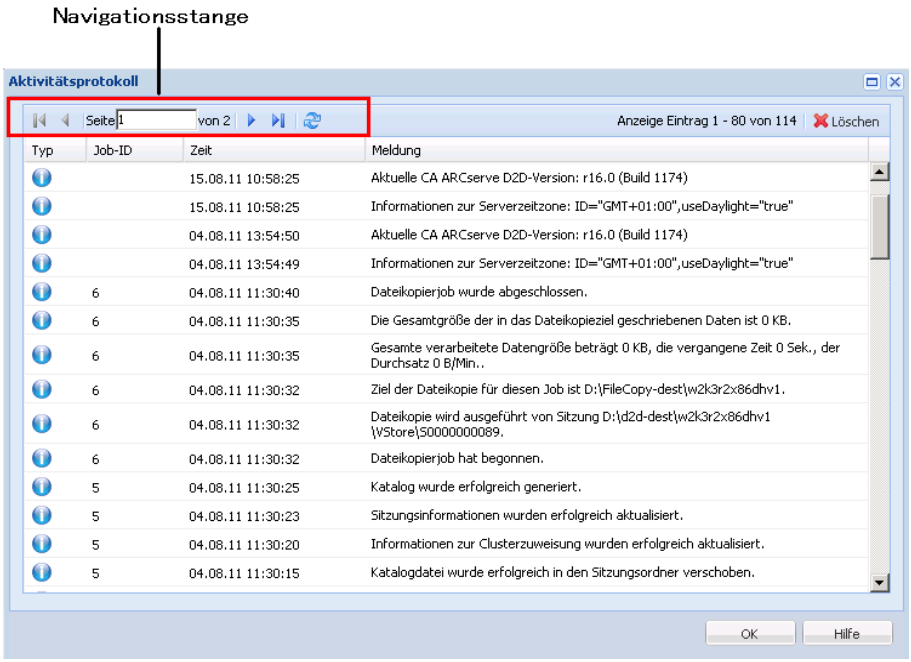
4. Klicken Sie auf die Registerkarte "Virtual Standby".

   Das Fenster "Übersicht über Virtual Standby" wird geöffnet.

5. (Optional) Wenn Sie auf einem Überwachungsserver angemeldet sind, blenden Sie in der Serverliste "Alle" oder "Server wird ausgeführt" ein, und klicken auf den Knoten, dessen Aktivitätsprotokolldaten Sie anzeigen möchten.

   Klicken Sie in der Aufgabenliste der virtuellen Konvertierung rechts im Fenster "Übersicht über Virtual Standby" auf "Protokolle anzeigen".

   Das Fenster "Aktivitätsprotokoll" wird geöffnet.


Navigationsstange
Aktivitätsprotokoll
Seite 1 von 2
Anzeige Eintrag 1 - 80 von 114
Löschen
Typ
Job-ID
Zeit
Meldung
15.08.11 10:58:25 Aktuelle CA ARCserve D2D-Version: r16.0 (Build 1174)
15.08.11 10:58:25 Informationen zur Serverzeitzone: ID="GMT+01:00",useDaylight="true"
04.08.11 13:54:50 Aktuelle CA ARCserve D2D-Version: r16.0 (Build 1174)
04.08.11 13:54:49 Informationen zur Serverzeitzone: ID="GMT+01:00",useDaylight="true"
6 04.08.11 11:30:40 Dateikopierjob wurde abgeschlossen.
6 04.08.11 11:30:35 Die Gesamtgröße der in das Dateikopieziel geschriebenen Daten ist 0 KB.
6 04.08.11 11:30:35 Gesamte verarbeitete Datengröße beträgt 0 KB, die vergangene Zeit 0 Sek., der Durchsatz 0 B/Min..
6 04.08.11 11:30:32 Ziel der Dateikopie für diesen Job ist D:\FileCopy-dest\w2k3r2x86dhv1.
6 04.08.11 11:30:32 Dateikopie wird ausgeführt von Sitzung D:\d2d-dest\w2k3r2x86dhv1 \VStore\50000000089.
6 04.08.11 11:30:32 Dateikopierjob hat begonnen.
5 04.08.11 11:30:25 Katalog wurde erfolgreich generiert.
5 04.08.11 11:30:23 Sitzungsinformationen wurden erfolgreich aktualisiert.
5 04.08.11 11:30:20 Informationen zur Clusterzuweisung wurden erfolgreich aktualisiert.
5 04.08.11 11:30:15 Katalogdatei wurde erfolgreich in den Sitzungsordner verschoben.
OK
Hilfe

   Verwenden Sie die Navigationsleiste, um nach Aktivitätsprotokolldatensätzen zu suchen und sie anzuzeigen. Die folgenden Symbole werden auf dem Aktivitätsprotokoll angezeigt:

   Informationen

   Warnung

   Fehler

   Hinweis: Informationen darüber, wie Sie Aktivitätsprotokolldatensätze löschen, finden Sie unter Löschen von Aktivitätsprotokolldatensätzen (siehe Seite 96).

Löschen von Aktivitätsprotokolldatensätzen

Virtual Standby lässt Sie die Gesamtgröße von Aktivitätsprotokolldaten verwalten. Das Aktivitätsprotokoll enthält Job-Datensätze für die von Ihnen geschützten CA ARCserve D2D-Quellknoten. Wenn Sie eine große Anzahl an Quellservern schützen oder häufig Sicherungen durchführen, kann das Aktivitätsprotokoll sehr viel Festplattenspeicher auf dem CA ARCserve D2D-Knoten in Anspruch nehmen.

Sie können Aktivitätsprotokolldatensätze, die älter sind als ein festgelegtes Datum, oder alle Aktivitätsprotokolldatensätze löschen.

Hinweis: Das Aktivitätsprotokoll (activity.log) wird im folgenden Verzeichnis auf dem Server gespeichert, in dem CA ARCserve D2D installiert ist:

```
C:\Programme\CA\ARCserve D2D\Protokolle
```

So löschen Sie Aktivitätsprotokolldatensätze

1. Öffnen Sie "Virtual Standby", und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   CA ARCserve D2D wird geöffnet.

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

4. Klicken Sie auf die Registerkarte "Virtual Standby".

   Das Fenster "Übersicht über Virtual Standby" wird geöffnet.

5. (Optional) Wenn Sie auf einem Überwachungsserver angemeldet sind, blenden Sie in der Serverliste "Alle" oder "Server wird ausgeführt" ein, und klicken auf den Knoten, dessen Aktivitätsprotokolldaten Sie löschen möchten.

6. Klicken Sie in der Aufgabenliste der virtuellen Konvertierung rechts im Fenster "Übersicht über Virtual Standby" auf "Protokolle anzeigen".

   Das Fenster "Aktivitätsprotokoll" wird geöffnet.

7. Klicken Sie in der Symbolleiste auf "Löschen".

   Das Dialogfeld "Aktivitätsprotokoll löschen" wird geöffnet.

8. Aktivieren Sie eine der folgenden Optionen:

   - **Alle Protokolldatensätze löschen:** Lässt Sie alle Jobdatensätze im Aktivitätsprotokoll löschen.

     Hinweis: Diese Option sollte mit Vorsicht verwendet werden. Sie können gelöschte Aktivitätsprotokolldatensätze nicht wiederherstellen.

   - **Alle Protokolldatensätze löschen, die älter sind als:** Lässt Sie alle Jobdatensätze im Aktivitätsprotokoll löschen, die älter sind als das Datum, das Sie festlegen.

   Klicken Sie auf "OK".

Die Datensätze werden aus dem Aktivitätsprotokoll gelöscht.

Anzeigen von Statusinformationen zu Virtual Standby-Jobs vom Virtual Standby-Server aus

CA ARCserve Central Virtual Standby konvertiert
CA ARCserve D2D-Wiederherstellungspunkte in Wiederherstellungspunkt-Snapshots. Sie können Statusinformationen zu momentan ausgeführten Virtual Standby-Jobs anzeigen.

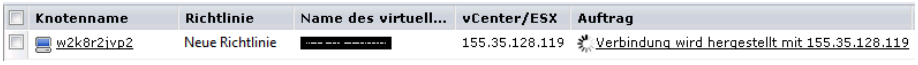
Optional können Sie vom Virtual Standby-Server oder direkt vom Knoten aus auf die Statusinformationen zugreifen. Weitere Informationen dazu, wie Sie von Knoten aus auf Statusinformationen zugreifen können, finden Sie unter Anzeigen von Statusinformationen zu Virtual Standby-Jobs von Knoten aus (siehe Seite 98).

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Virtual Standby-Server an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Wenn sich in Bearbeitung befindende Virtual Standby-Jobs vorliegen, wird die Phase des Jobs im Feld "Job" angezeigt, wie im folgenden Fenster veranschaulicht:



3. Klicken Sie auf die Phase, um das Dialogfeld "Statusüberwachung für Virtual Standby" zu öffnen.

   Hinweis: Weitere Informationen zu den Feldern, die in der Statusüberwachung für Virtual Standby angezeigt werden, finden Sie unter "Statusüberwachung für Virtual Standby" (siehe Seite 99).

4. Klicken Sie auf "Schließen", um das Dialogfeld "Statusüberwachung für Virtual Standby" zu schließen.

Anzeigen von Statusinformationen zu Virtual Standby-Jobs von Knoten aus

CA ARCserve Central Virtual Standby konvertiert
CA ARCserve D2D-Wiederherstellungspunkte in Wiederherstellungspunkt-Snapshots. Sie können Statusinformationen zu momentan ausgeführten Konvertierungsjobs anzeigen.

Optional können Sie vom Virtual Standby-Server oder direkt vom Knoten aus auf die Statusinformationen zugreifen. Weitere Informationen dazu, wie Sie vom Virtual Standby-Server aus auf Statusinformationen zugreifen können, finden Sie unter Anzeigen von Statusinformationen zu Virtual Standby-Jobs vom Virtual Standby-Server aus (siehe Seite 97).

Gehen Sie wie folgt vor:

1. Öffnen Sie die Anwendung und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

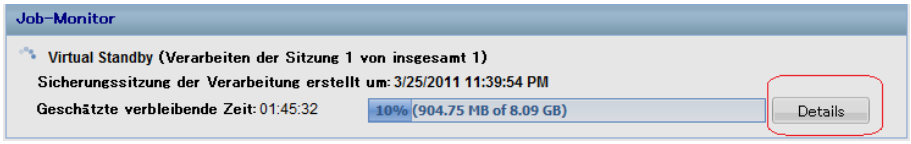
   Sie sind beim CA ARCserve D2D-Knoten angemeldet.

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

4. Klicken Sie auf die Registerkarte "Virtual Standby".

   Das Fenster "Übersicht über Virtual Standby" wird geöffnet.

   Wenn derzeit ein Virtual Standby-Job ausgeführt wird, öffnet sich im Feld "Job-Monitor", wie in der folgenden Abbildung veranschaulicht, ein Statusdialog:

   
   Job-Monitor
Virtual Standby (Verarbeiten der Sitzung 1 von insgesamt 1)
Sicherungssitzung der Verarbeitung erstellt um: 3/25/2011 11:39:54 PM
Geschätzte verbleibende Zeit: 01:45:32
10% (904.75 MB of 8.09 GB)
Details

5. Klicken Sie auf "Detail", um die "Statusüberwachung für Virtual Standby" zu öffnen.

   Hinweis: Weitere Informationen zu den Feldern, die in der Statusüberwachung für Virtual Standby angezeigt werden, finden Sie unter "Statusüberwachung für Virtual Standby" (siehe Seite 99).

6. Klicken Sie auf "Schließen", um das Dialogfeld "Statusüberwachung für Virtual Standby" zu schließen.

Statusüberwachung für Virtual Standby

Die Statusüberwachung für Virtual Standby wird geöffnet, um folgende Informationen zum Virtual Standby-Job in Echtzeit anzuzeigen:

Phase

Zeigt die aktuelle Phase des Konvertierungsprozesses an.

Job abbrechen

Job abbrechen: Ermöglicht es Ihnen, den Konvertierungsjob zu beenden.

Verarbeitung wird ausgeführt

Zeigt den Gesamtfortschritt des Konvertierungsjobs und die Sitzungsnummer des Wiederherstellungspunkts, den die Anwendung konvertiert, an.

Derzeitiger Bereitstellungspunkt

Zeigt Statusinformationen zur Sitzung an, die von der Anwendung konvertiert wird.

Quellsitzungen

Gibt die Sitzungsnummer der Sitzung an, die von der Anwendung konvertiert wird.

Startzeit

Zeigt das Datum und die Uhrzeit an, an denen die Anwendung die Sitzungskonvertierung gestartet hat.

Vergangene Zeit

Zeigt die Dauer der Zeit an, die vergangen ist, seitdem die Anwendung die Konvertierung der aktuellen Sitzung gestartet hat.

Durchsatz

Zeigt die Geschwindigkeit an, mit der die Anwendung die Sitzung konvertiert.

Geschätzte verbleibende Zeit

Zeigt die geschätzte Zeit an, die verbleibt, um die aktuelle Quellsitzung zu konvertieren.

Alle Sitzungen

Zeigt Statusinformationen für alle Sitzungen im Wiederherstellungspunkt an, die die Anwendung gerade konvertiert.

Anzahl der konvertierten Sitzungen

Zeigt die Gesamtzahl der Sitzungen im Bereitstellungspunkt an, die konvertiert wurden.

Vergangene Zeit

Zeigt die Zeitdauer an, die vergangen ist, seitdem die Anwendung die Konvertierung aller Sitzungen im Bereitstellungspunkt gestartet hat.

Geschätzte verbleibende Zeit

Zeigen Sie die geschätzte Zeitdauer an, die verbleibt, um alle im Wiederherstellungspunkt enthaltenen Sitzungen zu konvertieren.

Anzahl ausstehender Sitzungen

Zeigt die Anzahl von Sitzungen an, die zur Konvertierung ausstehen.

Anzeigen von Informationen über zu CA ARCserve D2D-Knoten zugewiesenen Richtlinien

Die Anwendung ermöglicht es Ihnen, Informationen zu den Konvertierungsrichtlinien anzuzeigen, die zu CA ARCserve D2D-Knoten zugewiesen sind.

So zeigen Sie Informationen über zu CA ARCserve D2D-Knoten zugewiesenen Richtlinien an

1. Öffnen Sie die Anwendung und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   Sie sind beim CA ARCserve D2D-Knoten angemeldet.

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

4. Klicken Sie auf die Registerkarte "Virtual Standby".

   Das Fenster "Übersicht über Virtual Standby" wird angezeigt.

5. Klicken Sie in der Aufgabenliste für Virtual Standby auf "Virtual Standby-Einstellungen".

   Das Dialogfeld "Virtual Standby-Einstellungen" wird geöffnet.

   Im Dialogfeld "Virtual Standby-Einstellungen" können Sie Informationen zum Virtualisierungsserver, dem virtuellen Rechner, dem Aushilfsserver und den Voreinstellungen anzeigen, die in der dem CA ARCserve D2D-Knoten zugewiesenen Richtlinie definiert sind. Sie können die Richtlinien, die zu CA ARCserve D2D zugewiesen sind, nicht im Dialogfeld "Virtual Standby-Einstellungen" bearbeiten.

   Hinweis: Informationen zum Bearbeiten von Richtlinien finden Sie unter Bearbeiten von Richtlinien (siehe Seite 60).

6. Klicken Sie auf "Abbrechen", um Dialogfeld "Virtual Standby-Einstellungen" zu schließen.

Einstellungen von Virtual Standby

Das Dialogfeld "Virtual Standby-Einstellungen" enthält Informationen über die Richtlinie, die dem Knoten zugewiesen ist. Sie können in diesem Dialogfeld keine Richtlinien bearbeiten. Weitere Informationen finden Sie unter Bearbeiten von Richtlinien (siehe Seite 60).

Auf der Registerkarte "Virtual Standby" werden die folgenden Optionen angezeigt:

Optionen für Virtualisierungsserver

- **VMware-Systeme:**

  Die folgenden Optionen sind auf VMware-Systemen anwendbar:

  - **Virtualisierungstyp:** VMware.
  - **ESX-Host/-Virtual Center**: Legt den Hostnamen des ESX- oder vCenter Server-Systems fest.
  - **Benutzername:** Legt den Benutzernamen fest, der für die Anmeldung beim VMware-System erforderlich ist.
  - **Kennwort:** Legt fest, dass für die Anmeldung beim VMware-System ein Kennwort für den Benutzernamen erforderlich ist.
  - **Protokoll:** Zeigt das Kommunikationsprotokoll an, das zwischen dem CA ARCserve D2D-Quellknoten und dem Überwachungsserver verwendet wird.
  - **Port:** Legt den Port fest, der für den Datentransfer zwischen dem Quellserver und dem Überwachungsserver verwendet wird.

- **Überwachung:**

  Die folgenden Optionen sind auf VMware-Systemen anwendbar.

  - **Überwachungsserver:** Legt den Hostnamen des Servers fest, der den Quellserver überwacht.
  - **Benutzername:** Legt den Benutzernamen fest, der für die Anmeldung beim Überwachungsserver erforderlich ist.
  - **Kennwort:** Legt fest, dass für die Anmeldung beim Überwachungsserver ein Kennwort für den Benutzernamen erforderlich ist.
  - **Protokoll:** Legt das Kommunikationsprotokoll fest, das zwischen dem CA ARCserve Central Virtual Standby-Server und dem ESX Server-System (dem Überwachungsserver) verwendet wird.
  - **Port:** Legt den Port fest, der für den Datentransfer zwischen dem CA ARCserve Central Virtual Standby-Server und dem ESX-Server-System (dem Überwachungsserver) verwenden möchten.
  - **Überwachungsserver als Proxy für den Datentransfer verwenden:** Legt fest, dass der Überwachungsserver die Konvertierungsdaten vom CA ARCserve D2D-Quellserver zum ESX-Server-Datenspeicher kopiert.

    Hinweis: Die Option "Überwachungsserver als Proxy für den Datentransfer verwenden" ist standardmäßig aktiviert. Sie können diese Option deaktivieren, um es dem CA ARCserve D2D-Quellserver zu ermöglichen, die Konvertierungsdaten direkt zum ESX-Server-Datenspeicher zu kopieren.

- **Hyper-V-Systeme:**

  Die folgenden Optionen sind auf Hyper-V-Systemen anwendbar:

  - **Virtualisierungstyp:** Hyper-V.
  - **Hyper-V-Hostname:** Legt den Hostnamen des Hyper-V-Systems fest.
  - **Benutzername:** Legt den Benutzernamen fest, der für die Anmeldung beim Hyper-V-System erforderlich ist.
  - **Kennwort:** Legt fest, dass für die Anmeldung beim Hyper-V-System ein Kennwort für den Benutzernamen erforderlich ist.
  - **Port:** Legt den Port fest, der für den Datentransfer zwischen dem Quellserver und dem Überwachungsserver verwendet wird.

Optionen für virtuelle Rechner

- **VMware-Systeme:**

  - **Präfix des Namens des virtuellen Rechners:** Legt den Anzeigenamen für den virtuellen Rechner auf dem ESX-Server-System fest.

    Standardwert: CAVM_
  - **VM-Ressourcenpool:** Legt den Namen des Ressourcenpools fest, zu dem der virtuelle Rechner in Standby-Zustand gehört.

- **Datenspeicher:** Legt den Speicherort fest, an dem Sie die Konvertierungsdaten speichern möchten.
  - **Verwenden Sie einen Datenspeicher für den gesamten Quelldatenträger des virtuellen Rechners:** Legt fest, dass die Anwendung alle Datenträger, die sich auf den virtuellen Rechner beziehen, in einen Datenspeicher kopiert.
  - **Wählen Sie einen Datenspeicher für jeden Quelldatenträger des virtuellen Rechners:** Legt fest, dass die Anwendung, datenträgerbezogene Informationen für den virtuellen Rechner in den entsprechenden Datenspeicher kopiert.
- **Netzwerke**: Definiert die NICs, virtuellen Netzwerke und Pfade, die das ESX-Server-System verwendet, um mit den virtuellen Rechnern zu kommunizieren.
  - **Verbinden Sie alle virtuellen NICs mit folgendem virtuellen Netzwerk**: Identifiziert die virtuellen NICs, die zum virtuellen Netzwerk zugeordnet sind. Diese Option ist aktiviert, wenn der virtuelle Rechner virtuelle NICs und ein virtuelles Netzwerk enthält.
  - **Wählen Sie ein virtuelles Netzwerk für jede virtuelle NIC**: Legt den Namen des virtuellen Netzwerks fest, das die NIC für Kommunikationszwecke verwenden soll.
- **CPU-Anzahl:** Legt die minimale und maximale CPU-Anzahl an, die vom virtuellen Rechner in Standby-Zustand unterstützt wird.
- **Speicher:** Legt die Gesamtgröße des RAM in MB fest, der für den virtuellen Rechner in Standby-Zustand zugewiesen werden soll.

- **Hyper-V-Systeme:**
  - **Präfix des Namens des virtuellen Rechners:** Legt den Anzeigenamen für den virtuellen Rechner auf dem Hyper-V-System fest.

    Standardwert: CAVM_
  - **Pfad:** Legt den Speicherort der Konvertierungsdaten auf dem Hyper-V Server fest.
  - **Netzwerke**: Definiert die NICs, virtuellen Netzwerke und Pfade, die der Hyper-V-Server verwendet, um mit den virtuellen Rechnern zu kommunizieren.
  - **CPU-Anzahl:** Legt die minimale und maximale CPU-Anzahl an, die vom virtuellen Rechner in Standby-Zustand unterstützt wird.
  - **Speicher:** Legt die Gesamtgröße des RAM in MB fest, der dem virtuellen Rechner in Standby-Zustand zugewiesen ist.

Aushilfseinstellungen

- **Wiederherstellung:**
  - **Virtuellen Rechner manuell starten**: Legt fest, dass die virtuellen Rechner manuell eingeschaltet und bereitgestellt werden, wenn der Quellserver fehlschlägt oder die Kommunikation mit dem Quellserver abbricht.
  - **Virtuellen Rechner automatisch starten**: Legt fest, dass die virtuellen Rechner automatisch eingeschaltet und bereitgestellt werden, wenn der Quellserver fehlschlägt oder die Kommunikation mit dem Quellserver abbricht.
- **Eigenschaften der Heartbeat-Signale:**
  - **Zeitlimit**: Gibt die Dauer der Zeit an, die der Überwachungsserver ein Heartbeat-Signal abwarten muss, bevor er einen Wiederherstellungspunkt-Snapshot einschaltet.
  - **Häufigkeit**: Legt die Häufigkeit fest, mit der der Quellserver ein Heartbeat-Signal an den Überwachungsserver sendet.

Auf der Registerkarte "Voreinstellungen" werden die folgenden Optionen angezeigt:

- **E-Mail-Warnmeldungen:**
  - **Fehlendes Heartbeat-Signal für Quellrechner:** Legt fest, dass Virtual Standby Warnmeldungen sendet, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver erkennt.
  - **VM eingeschaltet für Quellrechner, der mit automatischer Einschaltung konfiguriert ist:** Legt fest, dass Virtual Standby Warnmeldungen sendet, wenn ein virtueller Rechner eingeschaltet wird, der so konfiguriert wurde, dass eine automatische Inbetriebnahme erfolgt, wenn kein Heartbeat-Signal entdeckt wird.
  - **Fehlendes Heartbeat-Signal für Quellrechner, der für manuelles Einschalten konfiguriert ist:** Legt fest, dass Virtual Standby Warnmeldungen sendet, wenn kein Heartbeat-Signal von einem Quellserver erkannt wird, der nicht zur automatischen Inbetriebnahme konfiguriert ist.
  - **Freier VM-Speicherplatz beträgt weniger als:** Legt fest, dass Virtual Standby Warnmeldungen sendet, wenn auf dem angegebenen Hypervisor-Pfad nicht genügend freier Speicherplatz entdeckt wird. Dies tritt auf, wenn der freie Speicherplatz weniger ist als der benutzerdefinierte Schwellenwert. Der Schwellenwert kann entweder als absoluter Wert (MB) oder als prozentualer Anteil an der Gesamtkapazität angegeben werden.
  - **Virtual Standby-Fehler/-Ausfall/-Absturz:** Legt fest, dass Virtual Standby Warnmeldungen sendet, wenn ein Fehler entdeckt wird, der während des Konvertierungsprozesses aufgetreten ist.
  - **Virtual Standby-Erfolg**: Zeigt an, dass der Prozess des Erstellens eines virtuellen Virtual Standby-Rechners erfolgreich abgeschlossen wurde.

- **Hypervisor ist nicht erreichbar:** Legt fest, dass Virtual Standby Warnmeldungen sendet, wenn festgestellt wird, dass mit dem ESX-Server-System oder dem Hyper-V-System keine Kommunikation möglich ist.
- **Lizenzfehler:** Legt fest, dass Virtual Standby Warnmeldungen sendet, wenn Lizenzierungsprobleme auf Virtual Standby-Servern, Quellservern und Überwachungsservern festgestellt werden.
- **Virtual Standby wurde nicht erfolgreich vom Wiederherstellungspunkt-Snapshot gestartet** Zeigt an, dass der Prozess des Erstellens eines virtuellen Virtual Standby-Rechners von einem Wiederherstellungspunkt-Snapshot aus nicht erfolgreich abgeschlossen wurde.

So schützen Sie virtuelle Virtual Standby-Rechner

Nachdem ein virtueller Virtual Standby-Rechner eingeschaltet wurde (entweder manuell oder automatisch), werden der CA ARCserve D2D-Sicherungsjob und der Virtual Standby-Job nicht ausgeführt, da sie geplant wurden. Wenn Sie die Jobs nach dem Einschalten des virtuellen Virtual Standby-Rechners wiederaufnehmen möchten, gehen Sie folgendermaßen vor:

1. Ändern Sie das Präfix des Namens des virtuellen Rechners in der Virtual Standby-Richtlinie.

   Wenn CA ARCserve Central Virtual Standby virtuelle Virtual Standby-Rechner einschaltet, definiert die Anwendung die virtuellen Rechnernamen aus den eingeschalteten virtuellen Rechnern als Verknüpfung aus der Option "Präfix des Namens des virtuellen Rechners", die in der Virtual Standby-Richtlinie angegebenen ist, und dem Hostnamen des Quellknotens.

   Beispiel:

   - Präfix des Namens des virtuellen Rechners: AA_
   - Hostname des Quellknotens: Server1
   - Virtueller Rechnername des virtuellen Virtual Standby-Rechners: AA_Server1

   Wenn Sie das Präfix des Namens des virtuellen Rechners nicht in der Virtual Standby-Richtlinie ändern, können nach dem Einschalten der virtuellen Virtual Standby-Rechner Namenskonflikte bei virtuellen Rechnern auftreten. Probleme dieser Art treten auf, wenn sich die Quellknoten und die virtuellen Virtual Standby-Rechner auf dem gleichen Hypervisor befinden.

   Weitere Informationen darüber, wie das Präfix des Namens des virtuellen Rechners in der Virtual Standby-Richtlinie geändert werden kann, finden Sie unter Bearbeiten von Richtlinien (siehe Seite 60). Im Bedarfsfall können Sie andere Einstellungen der Virtual Standby-Richtlinien aktualisieren. Optional können Sie eine neue Virtual Standby-Richtlinie erstellen, um den virtuellen Virtual Standby-Rechner zu schützen. Weitere Information über das Erstellen neuer Richtlinien finden Sie unter Erstellen von Richtlinien (siehe Seite 32).

2. Nachdem Sie die Richtlinie aktualisiert oder eine neue Richtlinie erstellt haben, stellen Sie die Richtlinie für den virtuellen Virtual Standby-Rechner bereit. Weitere Informationen finden Sie unter Bereitstellen von Richtlinien (siehe Seite 40).
3. Nachdem Sie die Richtlinie für den virtuellen Virtual Standby-Rechner bereitgestellt haben, nehmen Sie den Virtual Standby-Job wieder auf. Weitere Informationen finden Sie unter Aussetzen und Wiederaufnehmen von Virtual Standby-Jobs (siehe Seite 87).
4. Nachdem Sie die Richtlinie bereitgestellt haben, melden Sie sich bei CA ARCserve D2D auf dem virtuellen Virtual Standby-Rechner an, und planen Sie eine Wiederholungsmethode für den CA ARCserve D2D-Sicherungsjob. Weitere Informationen finden Sie im *CA ARCserve D2D-Benutzerhandbuch*.

Hinweis: CA ARCserve Central Protection Manager und CA ARCserve Central Virtual Standby verfügen über einen Mechanismus, der es Ihnen ermöglicht, die Richtlinien für die verwalteten CA ARCserve D2D-Knoten wöchentlich neu zu synchronisieren. Mit diesem Mechanismus kann CA ARCserve Central Protection Manager die Sicherungsjobs auf den virtuellen Virtual Standby-Rechnern neu starten, indem die Richtlinie, die auf dem CA ARCserve D2D-Knoten effektiv war, erneut für den virtuellen Virtual Standby-Rechner bereitgestellt wird. Die Richtlinienbereitstellung verhält sich so, da der Quellknoten und der virtuelle Virtual Standby-Rechner den gleichen Hostnamen haben, was dazu führt, dass CA ARCserve Central Protection Manager die Richtlinie neu synchronisiert. Die einzige Einschränkung zu diesem Verhalten ist, der CA ARCserve Central Protection Manager-Server und der virtuelle Virtual Standby-Rechner müssen über das Netzwerk miteinander kommunizieren können. Nachdem CA ARCserve Central Protection Manager die Richtlinie neu synchronisiert und für den virtuellen Virtual Standby-Rechner bereitgestellt wurde, nehmen Sie dann den Virtual Standby-Job auf dem virtuellen Virtual Standby-Rechner wieder auf. Weitere Informationen finden Sie unter Aussetzen und Wiederaufnehmen von Virtual Standby-Jobs (siehe Seite 87).

Wiederherstellen von Daten aus CA ARCserve D2D-Wiederherstellungspunkten

Mit Virtual Standby können Sie Daten von den verfügbaren Wiederherstellungspunkten wiederherstellen. Die Wiederherstellungspunkte sind Daten-Snapshots für einen bestimmten Zeitpunkt, die sich auf CA ARCserve D2D-Quellknoten befinden. Aus den Wiederherstellungspunkten können Sie die Daten festlegen, die Sie wiederherstellen wollen.

So stellen Sie Daten aus CA ARCserve D2D-Wiederherstellungspunkten wieder her

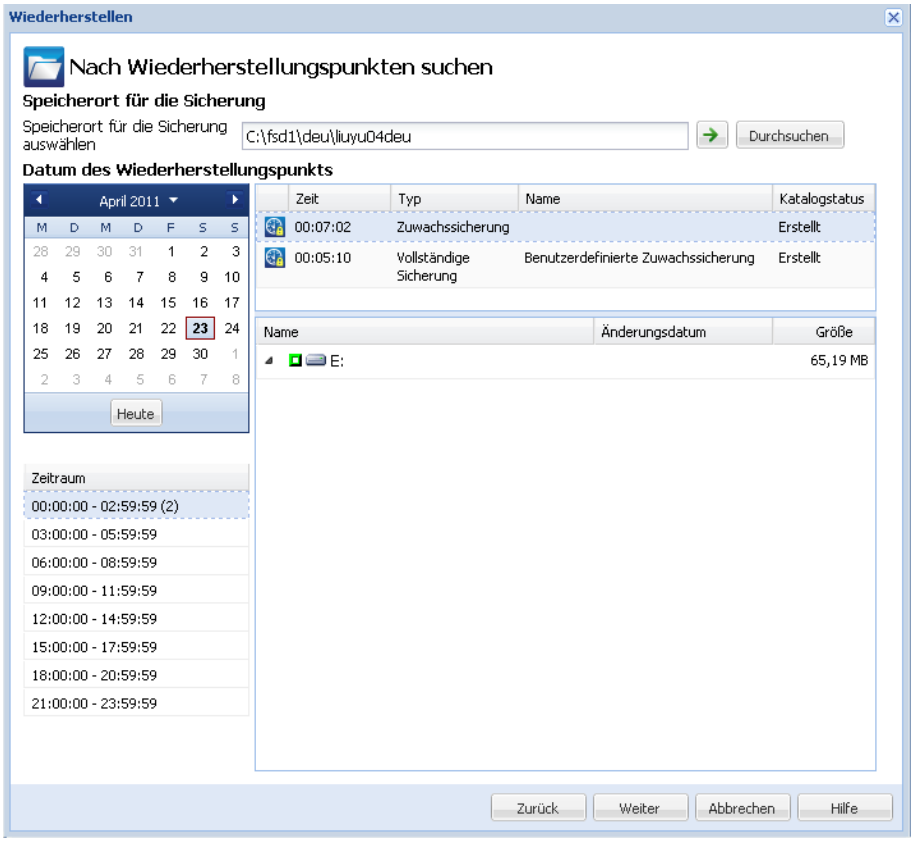
1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".

2. Klicken Sie im Dialogfeld "Wiederherstellen" auf "Wiederherstellungspunkte durchsuchen".

   Das Dialogfeld "Wiederherstellungspunkte durchsuchen" wird angezeigt.



3. Geben Sie die Sicherungsquelle an. Sie können den Speicherort der Sicherungs-Images angeben oder das System danach durchsuchen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten. Klicken Sie auf das grüne Pfeilsymbol, um zu überprüfen, ob ein ordnungsgemäßer Zugriff auf den Speicherort der Sicherungsquelle besteht.

   Im Kalender sind alle Daten für die angezeigte Zeitspanne, die Wiederherstellungspunkte für diese Sicherungsquelle enthalten, grün hervorgehoben.

4. Bestimmen Sie die Daten, die Sie wiederherstellen möchten.

   a. Geben Sie das Datum für das Sicherungs-Image an, das Sie wiederherstellen möchten.

      Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp und Name der Sicherung angezeigt.

   b. Wählen Sie einen Wiederherstellungspunkt aus, den Sie wiederherstellen möchten.

      Die entsprechenden Sicherungsinhalte (einschließlich Anwendungen) für diesen Wiederherstellungspunkt werden angezeigt.

      Hinweis: Eine Uhr mit einem Sperrsymbol zeigt an, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt.

   c. Wählen Sie die Inhalte aus, die wiederhergestellt werden sollen.

      - Bei einer Wiederherstellung auf Volume-Ebene können Sie angeben, ob das gesamte Volume oder ausgewählte Dateien/Ordner wiederhergestellt werden sollen.
      - Bei einer Wiederherstellung auf Anwendungsebene können Sie festlegen, ob die gesamte Anwendung, oder ausgewählte Komponenten, Datenbanken, Instanzen etc. wiederhergestellt werden sollen.

5. Nachdem Sie die wiederherzustellenden Daten angegeben haben, klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungsoptionen" wird geöffnet.

6. Füllen Sie im Dialogfeld "Wiederherstellungsoptionen" folgende Optionen aus:

   - **Ziel:** Wählen Sie das Ziel für die Wiederherstellung aus.

     - Am ursprünglichen Speicherort wiederherstellen: Ermöglicht es Ihnen, Dateien am ursprünglichen Speicherort wiederherzustellen, an dem das Sicherungs-Image erfasst wurde.

     - Wiederherstellen auf: Sie können einen Speicherort für die Wiederherstellung Ihrer Sicherungs-Images festlegen oder danach suchen. Klicken Sie auf den Pfeil neben dem Feld "Wiederherstellen auf", um die Verbindung zum angegebenen Speicherort zu überprüfen.

       Wenn erforderlich, müssen Sie Benutzername und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

   - **Konfliktlösung:** Lässt Sie festlegen, wie CA ARCserve D2D Konflikte lösen soll, die während der Wiederherstellung festgestellt werden.

     - Vorhandene Dateien überschreiben: Lässt Sie vorhandene Dateien überschreiben (ersetzen), die am Wiederherstellungsziel gefunden werden. Alle Objekte werden wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.

     - Aktive Dateien ersetzen: Ermöglicht es Ihnen, aktive Dateien nach Neustart zu ersetzen. Wenn CA ARCserve D2D während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

       Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.

     - Dateien umbenennen: Lässt Sie neue Dateien erstellen, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit dem gleichen Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten werden dann in einer neuen Datei wiederhergestellt.

     - Vorhandene Dateien überspringen: Lässt Sie alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, überspringen und nicht überschreiben (ersetzen). Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

       Standardmäßig ist diese Option aktiviert.

- **Verzeichnisstruktur:** Lässt Sie festlegen, was CA ARCserve D2D während der Wiederherstellung mit der Verzeichnisstruktur vornehmen wird oder nicht.
  - Stammverzeichnis erstellen: Lässt Sie festlegen, dass, falls eine Verzeichnisstruktur im erfassten Sicherungs-Image vorhanden ist, CA ARCserve D2D die gleiche Verzeichnisstruktur am Wiederherstellungszielpfad erstellt.

    Wenn die Option "Stammverzeichnis erstellen" nicht ausgewählt (deaktiviert) ist, werden die ausgewählten Dateien/Ordner direkt im Zielordner wiederhergestellt.

    Beispiel:

    Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

    Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).

    Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

    Wenn die Option "Stammverzeichnis erstellen" ausgewählt (aktiviert) ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich Volume-Name) im Zielordner wiederhergestellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

    Beispiel:

    Sie haben während der Sicherung die Dateien"C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

    Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).

Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

- **Verschlüsselungskennwort:** Wenn die Wiederherstellungspunktdaten, die Sie versuchen wiederherzustellen, verschlüsselt sind, müssen Sie möglicherweise das Verschlüsselungskennwort angeben.

  Ein Kennwort ist nicht erforderlich, wenn Sie versuchen, die Wiederherstellung auf dem gleichen Rechner durchzuführen, auf dem die verschlüsselte Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung auf einem anderen Rechner durchzuführen, ist ein Kennwort erforderlich.

  Hinweis: Die folgenden Symbole zeigen an, ob der Wiederherstellungspunkt verschlüsselte Informationen enthält, und können ein Kennwort zur Wiederherstellung benötigen.

  Nicht verschlüsselter Wiederherstellungspunkt

  Verschlüsselter Wiederherstellungspunkt

Klicken Sie auf "Weiter".

Das Dialogfeld "Wiederherstellungs-Übersicht" wird geöffnet.

7. Überprüfen Sie, ob die Informationen auf dem Dialogfeld "Wiederherstellungs-Übersicht" richtig sind.

   Hinweis: Wenn Sie die Wiederherstellungsoptionen, die Sie festgelegt haben, ändern wollen, klicken Sie auf "Zurück" und gehen Sie zum zutreffenden Dialogfeld, um die Werte zu ändern.

   Klicken Sie auf Fertig stellen.

Die Wiederherstellungsoptionen werden angewendet und die Daten werden wieder hergestellt.

Wiederherstellen von Daten aus CA ARCserve D2D-Dateikopien

Virtual Standby ermöglicht es Ihnen, Daten aus CA ARCserve D2D-Dateikopien wiederherzustellen. Dateikopien sind Kopien von CA ARCserve D2D-Wiederherstellungspunkten, die Sie zur Offline-Speicherung beispielsweise auf Festplatten oder in die Cloud kopieren. Aus den Dateikopien können Sie die Daten festlegen, die Sie wiederherstellen wollen.

So stellen Sie Daten aus CA ARCserve D2D-Dateikopien wieder her

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

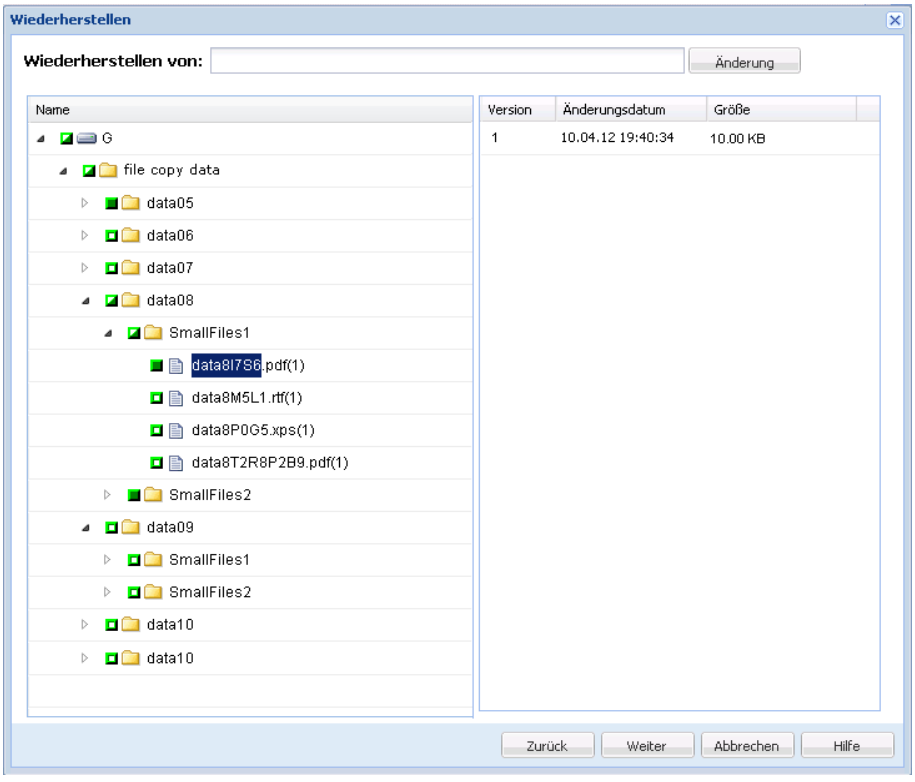
   Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".

2. Klicken Sie im Dialogfeld "Wiederherstellen" auf "Nach Dateikopien suchen".

   Das Dialogfeld "Dateikopien durchsuchen" wird geöffnet, wie im folgenden Dialogfeld gezeigt.

   Hinweis: Das Ziel, das im rechten Bereich angezeigt wird, ist das Standardziel.

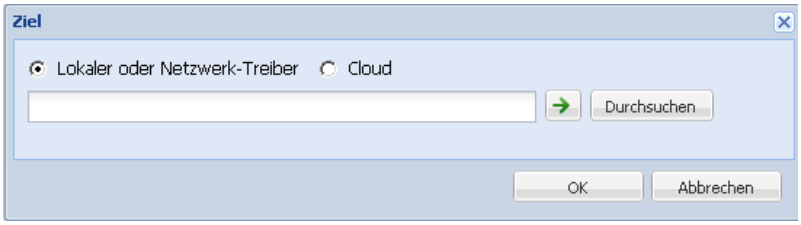


3. Geben Sie vom Bereich "Namen" aus die Daten der Dateikopie an, die Sie wiederherstellen wollen. Sie können eine beliebige Kombination aus Dateien und Ordnern oder dem Volume festlegen.

   Wenn Sie eine individuelle Datei zur Wiederherstellung auswählen, werden alle kopierten Versionen dieser Datei im rechten Bereich angezeigt. Wenn mehrere Versionen verfügbar sind, wählen Sie die Version der Dateikopie aus, die Sie wiederherstellen wollen.

   - **Ziel ändern:** Lässt Sie einen alternativen Speicherort suchen, an dem Ihre Dateikopie-Images gespeichert werden.

     Ein Dialogfeld öffnet sich und zeigt die verfügbaren alternativen Zieloptionen an.

   - **Lokaler oder Netzwerk-Treiber**: Das Dialogfeld "Speicherort für die Sicherung auswählen" wird geöffnet. Sie können einen alternativen Speicherort für Ihr lokales oder Netzwerklaufwerk suchen und auswählen.
   - **Cloud**: Das Dialogfeld "Cloud-Konfiguration" wird geöffnet und ermöglicht es Ihnen, auf einen alternativen Cloud-Speicherort zuzugreifen und ihn auszuwählen.

4. Klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungsoptionen" wird geöffnet.

5. Füllen Sie im Dialogfeld "Wiederherstellungsoptionen" folgende Optionen aus:

   - **Ziel:** Wählen Sie das Ziel für die Wiederherstellung aus.
     - Am ursprünglichen Speicherort wiederherstellen: Ermöglicht es Ihnen, Dateien am ursprünglichen Speicherort wiederherzustellen, an dem das Sicherungs-Image erfasst wurde.
     - Wiederherstellen auf: Sie können einen Speicherort für die Wiederherstellung Ihrer Sicherungs-Images festlegen oder danach suchen. Klicken Sie auf den Pfeil neben dem Feld "Wiederherstellen auf", um die Verbindung zum angegebenen Speicherort zu überprüfen.

       Wenn erforderlich, müssen Sie Benutzername und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

- **Konfliktlösung:** Lässt Sie festlegen, wie CA ARCserve D2D Konflikte lösen soll, die während der Wiederherstellung festgestellt werden.
  - Vorhandene Dateien überschreiben: Lässt Sie vorhandene Dateien überschreiben (ersetzen), die am Wiederherstellungsziel gefunden werden. Alle Objekte werden wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.
  - Aktive Dateien ersetzen: Ermöglicht es Ihnen, aktive Dateien nach Neustart zu ersetzen. Wenn CA ARCserve D2D während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

    Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.
  - Dateien umbenennen: Lässt Sie neue Dateien erstellen, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit dem gleichen Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten werden dann in einer neuen Datei wiederhergestellt.
  - Vorhandene Dateien überspringen: Lässt Sie alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, überspringen und nicht überschreiben (ersetzen). Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

    Standardmäßig ist diese Option aktiviert.

- **Verzeichnisstruktur:** Lässt Sie festlegen, was CA ARCserve D2D während der Wiederherstellung mit der Verzeichnisstruktur vornehmen wird oder nicht.
  - Stammverzeichnis erstellen: Lässt Sie festlegen, dass, falls eine Verzeichnisstruktur im erfassten Sicherungs-Image vorhanden ist, CA ARCserve D2D die gleiche Verzeichnisstruktur am Wiederherstellungszielpfad erstellt.

    Wenn die Option "Stammverzeichnis erstellen" nicht ausgewählt (deaktiviert) ist, werden die ausgewählten Dateien/Ordner direkt im Zielordner wiederhergestellt.

    Beispiel:

    Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

    Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).

    Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

    Wenn die Option "Stammverzeichnis erstellen" ausgewählt (aktiviert) ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich Volume-Name) im Zielordner wiederhergestellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

    Beispiel:

    Sie haben während der Sicherung die Dateien"C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

    Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).

Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

- **Verschlüsselungskennwort:** Wenn die Wiederherstellungspunktdaten, die Sie versuchen wiederherzustellen, verschlüsselt sind, müssen Sie möglicherweise das Verschlüsselungskennwort angeben.

  Ein Kennwort ist nicht erforderlich, wenn Sie versuchen, die Wiederherstellung auf dem gleichen Rechner durchzuführen, auf dem die verschlüsselte Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung auf einem anderen Rechner durchzuführen, ist ein Kennwort erforderlich.

  Hinweis: Die folgenden Symbole zeigen an, ob der Wiederherstellungspunkt verschlüsselte Informationen enthält, und können ein Kennwort zur Wiederherstellung benötigen.

  Nicht verschlüsselter Wiederherstellungspunkt

  Verschlüsselter Wiederherstellungspunkt

Klicken Sie auf "Weiter".

Das Dialogfeld "Wiederherstellungs-Übersicht" wird geöffnet.

6. Überprüfen Sie, ob die Informationen auf dem Dialogfeld "Wiederherstellungs-Übersicht" richtig sind.

   Hinweis: Wenn Sie die Wiederherstellungsoptionen, die Sie festgelegt haben, ändern wollen, klicken Sie auf "Zurück" und gehen Sie zum zutreffenden Dialogfeld, um die Werte zu ändern.

   Klicken Sie auf Fertig stellen.

Die Wiederherstellungsoptionen werden angewendet und die Daten werden wieder hergestellt.

Wiederherstellen von Daten mithilfe von "Wiederherzustellende Dateien/Ordner suchen"

Virtual Standby ermöglicht es Ihnen, CA ARCserve D2D-Wiederherstellungspunkte und Dateikopien für bestimmte Dateien oder wiederherzustellende Ordner zu suchen.

So stellen Sie Daten mithilfe von "Wiederherzustellende Dateien/Ordner suchen" wieder her

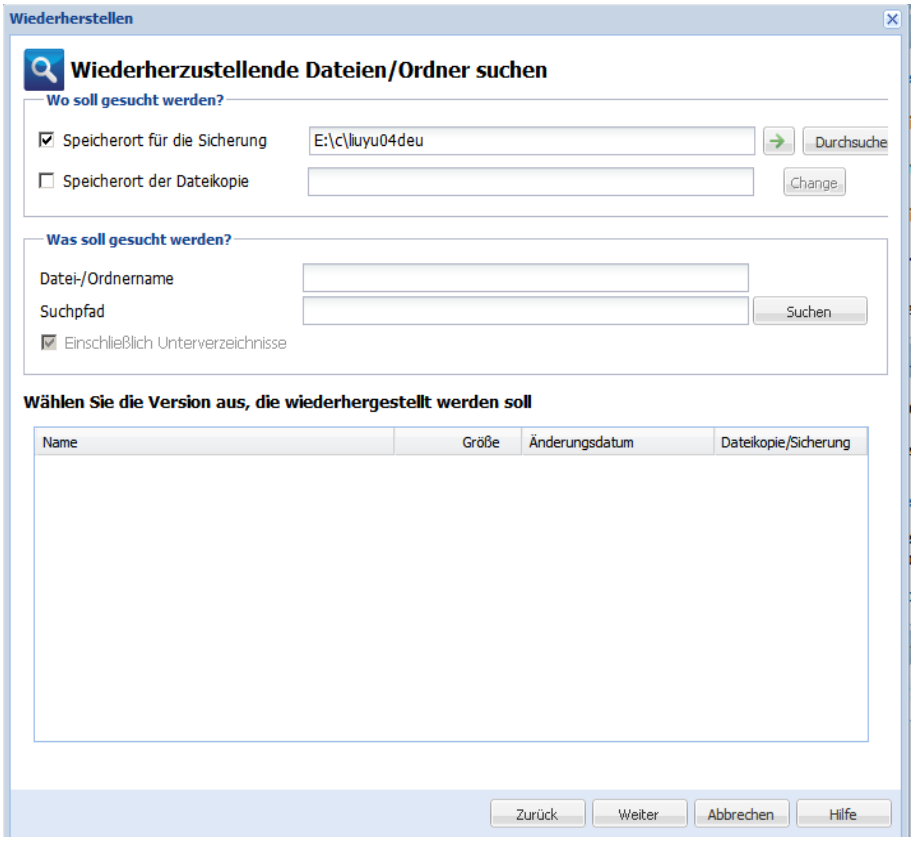
1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".

2. Klicken Sie im Dialogfeld "Wiederherstellen" auf "Wiederherzustellende Dateien/Ordner suchen".

   Das Dialogfeld "Wiederzustellende Dateien/Ordner suchen" wird geöffnet.



3. Geben Sie an, wo gesucht werden soll (Sicherungs- und/oder Archivquelle).

   Sie können den Speicherort der Sicherungs- oder Archiv-Images angeben oder das System danach durchsuchen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten. Klicken Sie auf das grüne Pfeilsymbol, um zu überprüfen, ob ein ordnungsgemäßer Zugriff auf den Speicherort der Sicherungsquelle besteht.

4. Geben Sie an, wonach gesucht werden soll (wiederherzustellender Datei- oder Ordnername).

   Hinweis: Das Feld "Dateiname" unterstützt die Suche nach vollständigen Namen oder mit Platzhaltern. Wenn Ihnen der vollständige Dateiname nicht bekannt ist, können Sie die Abfrage vereinfachen, indem Sie die Platzhalter "*" und "?" im Feld "Dateiname" eingeben.

   Folgende Platzhalter für den Datei- oder Ordnernamen werden unterstützt:

   - "*" - Verwenden Sie den Asterisk, um null oder mehr Zeichen in einem Datei- oder Ordnernamen zu ersetzen.
   - "?" - Verwenden Sie das Fragezeichen, um ein einzelnes Zeichen in einem Datei- oder Ordnernamen zu ersetzen.

   Beispiel: Wenn Sie *.txt angeben, werden alle Dateien mit einer .txt-Dateierweiterung in den Suchergebnissen angezeigt.

   Hinweis: Sie können Ihre Suche auch mit einer Pfadangabe filtern und angeben, ob Unterverzeichnisse in die Suche eingeschlossen werden sollen.

5. Klicken Sie auf "Suchen", um die Suche zu starten.

   Die Suchergebnisse werden angezeigt. Wenn mehrere Wiederherstellungspunkte für dieselbe Datei gefunden werden, werden alle Wiederherstellungspunkte nach Datum geordnet aufgelistet (der letzte steht an erster Stelle). Es wird außerdem angezeigt, ob die gesuchte Datei gesichert oder archiviert wurde.

6. Wählen Sie die Version (Ereignis) der Dateien oder Ordner aus, die Sie wiederherstellen möchten, und klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungsoptionen" wird geöffnet.

7. Füllen Sie im Dialogfeld "Wiederherstellungsoptionen" folgende Optionen aus:

   - **Ziel:** Wählen Sie das Ziel für die Wiederherstellung aus.
     - Am ursprünglichen Speicherort wiederherstellen: Ermöglicht es Ihnen, Dateien am ursprünglichen Speicherort wiederherzustellen, an dem das Sicherungs-Image erfasst wurde.
     - Wiederherstellen auf: Sie können einen Speicherort für die Wiederherstellung Ihrer Sicherungs-Images festlegen oder danach suchen. Klicken Sie auf den Pfeil neben dem Feld "Wiederherstellen auf", um die Verbindung zum angegebenen Speicherort zu überprüfen.

       Wenn erforderlich, müssen Sie Benutzername und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

- **Konfliktlösung:** Lässt Sie festlegen, wie CA ARCserve D2D Konflikte lösen soll, die während der Wiederherstellung festgestellt werden.
  - Vorhandene Dateien überschreiben: Lässt Sie vorhandene Dateien überschreiben (ersetzen), die am Wiederherstellungsziel gefunden werden. Alle Objekte werden wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.
  - Aktive Dateien ersetzen: Ermöglicht es Ihnen, aktive Dateien nach Neustart zu ersetzen. Wenn CA ARCserve D2D während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

    Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.
  - Dateien umbenennen: Lässt Sie neue Dateien erstellen, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit dem gleichen Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten werden dann in einer neuen Datei wiederhergestellt.
  - Vorhandene Dateien überspringen: Lässt Sie alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, überspringen und nicht überschreiben (ersetzen). Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

    Standardmäßig ist diese Option aktiviert.

- **Verzeichnisstruktur:** Lässt Sie festlegen, was CA ARCserve D2D während der Wiederherstellung mit der Verzeichnisstruktur vornehmen wird oder nicht.
  - Stammverzeichnis erstellen: Lässt Sie festlegen, dass, falls eine Verzeichnisstruktur im erfassten Sicherungs-Image vorhanden ist, CA ARCserve D2D die gleiche Verzeichnisstruktur am Wiederherstellungszielpfad erstellt.

    Wenn die Option "Stammverzeichnis erstellen" nicht ausgewählt (deaktiviert) ist, werden die ausgewählten Dateien/Ordner direkt im Zielordner wiederhergestellt.

    Beispiel:

    Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

    Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).

    Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

    Wenn die Option "Stammverzeichnis erstellen" ausgewählt (aktiviert) ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich Volume-Name) im Zielordner wiederhergestellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

    Beispiel:

    Sie haben während der Sicherung die Dateien"C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

    Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).

Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

- **Verschlüsselungskennwort:** Wenn die Wiederherstellungspunktdaten, die Sie versuchen wiederherzustellen, verschlüsselt sind, müssen Sie möglicherweise das Verschlüsselungskennwort angeben.

  Ein Kennwort ist nicht erforderlich, wenn Sie versuchen, die Wiederherstellung auf dem gleichen Rechner durchzuführen, auf dem die verschlüsselte Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung auf einem anderen Rechner durchzuführen, ist ein Kennwort erforderlich.

  Hinweis: Die folgenden Symbole zeigen an, ob der Wiederherstellungspunkt verschlüsselte Informationen enthält, und können ein Kennwort zur Wiederherstellung benötigen.

  Nicht verschlüsselter Wiederherstellungspunkt

  Verschlüsselter Wiederherstellungspunkt

Klicken Sie auf "Weiter".

Das Dialogfeld "Wiederherstellungs-Übersicht" wird geöffnet.

8. Überprüfen Sie, ob die Informationen auf dem Dialogfeld "Wiederherstellungs-Übersicht" richtig sind.

   Hinweis: Wenn Sie die Wiederherstellungsoptionen, die Sie festgelegt haben, ändern wollen, klicken Sie auf "Zurück" und gehen Sie zum zutreffenden Dialogfeld, um die Werte zu ändern.

   Klicken Sie auf Fertig stellen.

Die Wiederherstellungsoptionen werden angewendet und die Daten werden wieder hergestellt.

Wiederherstellen von Quellservern mithilfe von Bare-Metal-Recovery

Nachdem Sie die Probleme behoben oder Ihre Quellserver gewartet haben, können Sie mit Virtual Standby die Quellserver zu ihrem letzten gesunden Zustand wiederherstellen, und die inkrementellen Änderungen einschließen, die auftraten, während der Wiederherstellungspunkt-Snapshot in Betrieb war.

Dieser Wiederherstellungsprozess wird als V2P-Wiederherstellung bezeichnet (virtuell zu physisch).

Der V2P-Wiederherstellungsprozess analysiert die
CA ARCserve D2D-Bare-Metal-Recovery (BMR), um Daten von virtuellen Rechnern auf physischen Rechnern wiederherzustellen. BMR ist eine Wiederherstellung Ihres Computersystems "von Null" an, einschließlich des Betriebssystems und Anwendungen, mit einer darauffolgenden Wiederherstellung von Daten und Einstellungen.

Voraussetzungen für eine Bare-Metal-Recovery:

- Sie müssen über einen der folgenden Punkte verfügen:
  - Ein benutzerdefiniertes Windows PE-Image (D2DBMR.ISO), das über CA ARCserve D2D vertrieben wird.
  - Einen USB-Stick für BMR, der über den Bootkit-Assistenten erstellt wurde, sowie den Installationsdatenträger für Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 (CD/DVD). (Wenn erforderlich, kann der USB-Stick auch mit dem Windows PE-Image anstelle des Installationsdatenträgers verwendet werden, um die notwendigen Treiber während der BMR zu laden).

    Hinweis: Wenn Sie einen USB-Stick verwenden, können Sie zusätzliche Treiber hinzufügen, was Sie beim Windows PE-Image nicht können.
- Sie müssen über mindestens eine vollständige Sicherung verfügen.
- Auf dem virtuellen Rechner und auf dem Quellserver, den Sie wiederherstellen, muss mindestens 1 GB RAM installiert sein.
- Um virtuelle VMware-Rechner zu virtuellen VMware-Rechnern wiederherzustellen, die auf das Verhalten eines physischen Servers konfiguriert wurden, stellen Sie sicher, dass die Anwendung "VMware Tools" auf dem virtuellen Rechner des Ziels installiert ist.

Dynamische Datenträger werden nur auf Datenträgerebene wiederhergestellt. Wenn Ihre Daten auf einem lokalen Volume eines dynamischen Datenträgers gesichert sind, können Sie diesen dynamischen Datenträger während der Bare-Metal-Recovery nicht wiederherstellen. Um in diesem Szenario eine Wiederherstellung während der BMR durchzuführen, müssen Sie eine der folgenden Aufgaben ausführen, und dann eine BMR vom kopierten Wiederherstellungspunkt aus durchführen:

- Führen Sie eine Sicherung auf einem Volume oder auf einem anderen Laufwerk durch.
- Führen Sie eine Sicherung auf der Remote-Freigabe durch.
- Kopieren Sie einen Wiederherstellungspunkt in einen anderen Speicherort.

Hinweis: Wenn Sie BMR auf einem dynamischen Datenträger durchführen, führen Sie auf dem Datenträger keine Vorgänge vor der BMR aus (Volume reinigen oder löschen etc.), da der Datenträger ansonsten möglicherweise nicht erkannt wird.

Der Prozess der Bare-Metal-Recovery ist bei den beiden Arten der Erstellung des Bootkit-Images praktisch identisch.

Die Anwendung ermöglicht es Ihnen, Daten mithilfe der in der folgenden Tabelle beschriebenen Methoden wiederherzustellen:

Wiederherstellungsmethode	Weitere Informationen
Quellserver aus Daten wiederherstellen, die mithilfe von CA ARCserve D2D gesichert wurden.	Wiederherstellen von Quellservern mithilfe von CA ARCserve D2D-Sicherungsdaten (siehe Seite 124).
Quellserver aus Daten wiederherstellen, die in Hyper-V-basierte virtuelle Virtual Standby-Rechner konvertiert wurden.	Wiederherstellen von Quellservern mithilfe von Daten aus Hyper-V-basierten virtuellen Virtual Standby-Rechnern (siehe Seite 139).
Quellserver aus Daten wiederherstellen, die in VMware-basierte virtuelle Virtual Standby-Rechner konvertiert wurden.	Wiederherstellen von Quellservern mithilfe von Daten aus VMware-basierten virtuellen Virtual Standby-Rechnern (siehe Seite 153).

Wiederherstellen von Quellservern mithilfe von CA ARCserve D2D-Sicherungsdaten

Mit der Anwendung können Sie Quellserver aus Daten wiederherstellen, die mithilfe von CA ARCserve D2D gesichert wurden.

Hinweis: Die Anwendung verwendet den Bare-Metal-Recovery-Prozess, um Quellserver aus CA ARCserve D2D-Sicherungsdaten wiederherzustellen. Weitere Informationen finden Sie unter Wiederherstellen von Quellservern mithilfe von Bare-Metal-Recovery (siehe Seite 122).

So stellen Sie Quellserver mithilfe von CA ARCserve D2D-Sicherungsdaten wieder her

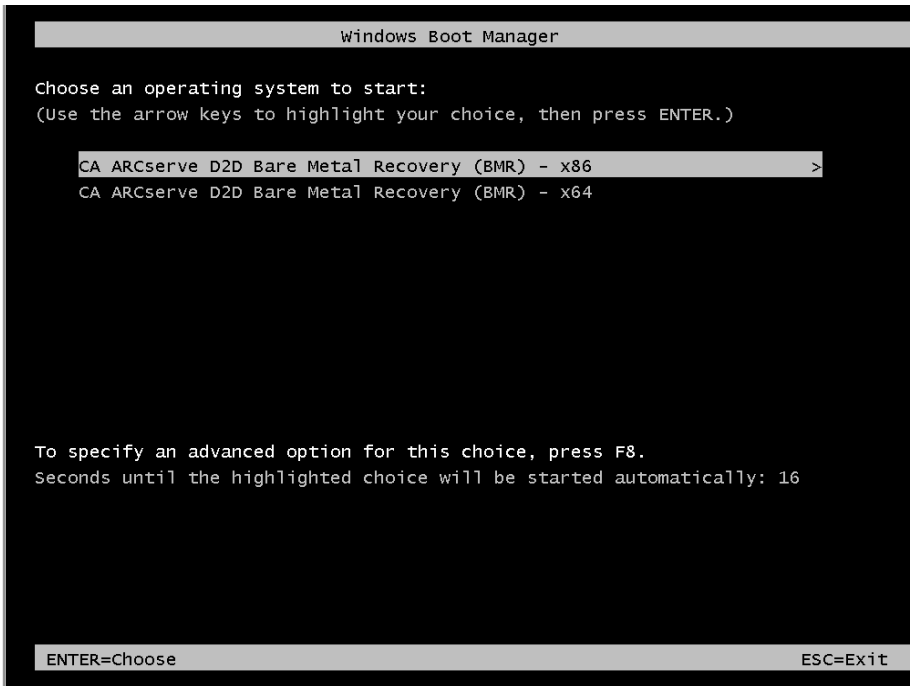
1. Legen Sie den Datenträger ein, auf dem das Bootkit-Image gespeichert ist, und starten Sie den Computer.

   - Wenn Sie ein abgespeichertes Windows Server PE-Image verwenden, legen Sie die entsprechende CD oder DVD ein.
   - Wenn Sie einen USB-Stick verwenden, legen Sie die Windows Server Installations-CD oder -DVD und anschließend den USB-Stick mit dem Bootkit-Image ein.

   Der Bildschirm des BIOS-Setup-Hilfsprogramms wird angezeigt.

2. Wählen Sie in diesem Bildschirm die Option "CD-ROM Drive", um den Neustart zu initiieren.

   Hinweis: Wenn Sie Windows PE-Image für BMR verwenden, müssen Sie eine Architektur (x86/x64) auswählen und auf "Eingabe" drücken, um fortzufahren.


Windows Boot Manager
Choose an operating system to start:
(Use the arrow keys to highlight your choice, then press ENTER.)
CA ARCserve D2D Bare Metal Recovery (BMR) - x86
CA ARCserve D2D Bare Metal Recovery (BMR) - x64
To specify an advanced option for this choice, press F8.
Seconds until the highlighted choice will be started automatically: 16
ENTER=Choose
ESC=Exit

3. Der CA ARCserve D2D-Bildschirm zur Sprachauswahl wird angezeigt. Wählen Sie eine Sprache aus und klicken Sie auf "Weiter", um fortzufahren.

   Hinweis: Wenn Sie BMR mit einem USB-Stick für BMR und einem Installationsdatenträger für
   Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 (CD/DVD)
   durchführen, der Multilingual User Interface (MUI) nicht unterstützt, wird der Bildschirm zur Sprachauswahl nicht angezeigt.

Die Bare-Metal-Recovery wird gestartet und der erste Bildschirm des BMR-Assistenten wird angezeigt.

ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wählen Sie einen BMR-Typ aus
Legen Sie einen Wiederherstellungstyp fest:
Gesicherte Daten mit CA ARCserve D2D wiederherstellen
(Sicherungssitzungen mit CA ARCserve D2D oder CA ARCserve Central Host-Based VM Backup).
Wiederherstellen mit einer Hyper-V-Virtual Standby-VM
(Sie können Daten nur wiederherstellen, wenn die virtuelle Konvertierung mit CA ARCserve Central Virtual Standby ausgeführt wurde)
Wiederherstellen mit einer VMware-Virtual Standby-VM
(Sie können Daten nur wiederherstellen, wenn die virtuelle Konvertierung mit CA ARCserve Central Virtual Standby ausgeführt wurde)
Hilfsprogramme
Zurück
Weiter
Abbrechen

4. Klicken Sie auf "Gesicherte Daten mit CA ARCserve D2D wiederherstellen" und dann auf "Weiter".

   Im Assistenten wird das Fenster "Wiederherstellungspunkt auswählen" angezeigt.

ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungspunkt auswählen
Im oberen Bereich werden alle gesicherten Rechner sowie deren Sicherungsziel angezeigt. Wenn Sie auf einen Rechner klicken, werden die entsprechenden Wiederherstellungspunkte im unteren Bereich angezeigt. Wählen Sie einen Wiederherstellungspunkt aus, um fortzufahren.
Hinweis: Standardmäßig werden hier nur die gesicherten Rechner aufgelistet, die auf lokalen Volumes gefunden wurden. Wenn Sie einen Wechseldatenträger hinzufügen oder entfernen, klicken Sie auf 'Aktualisieren', um die Liste der Rechner zu aktualisieren.
Um gesicherte Rechner vom freigegebenen Remote-Ordner hinzuzufügen, klicken Sie auf 'Durchsuchen'.
Wenn der freigegebene Remote-Ordner nicht durchsucht werden kann, ist möglicherweise der NIC-Treiber nicht installiert. oder die IP-
1 Netzwerkadapter gefunden
Microsoft Virtual Machine Bus Network Adapter
- IP-Adresse:
- Status: Verbunden
Folgende gesicherte Rechner wurden gefunden:
Informationen zum gesicherten Rechner
Hostname:
Betriebssystem:
Plattform:
Aktualisieren
Durchsuchen
Wählen Sie einen Wiederherstellungspunkt für den angegebenen Rechner aus, und fahren Sie fort:
Hilfsprogramme
Zurück
Weiter
Abbrechen

5. Wählen Sie im Fenster "Wiederherstellungspunkt auswählen" den Rechner (oder das Volume) aus, der Wiederherstellungspunkte für Ihr Sicherungs-Image enthält.

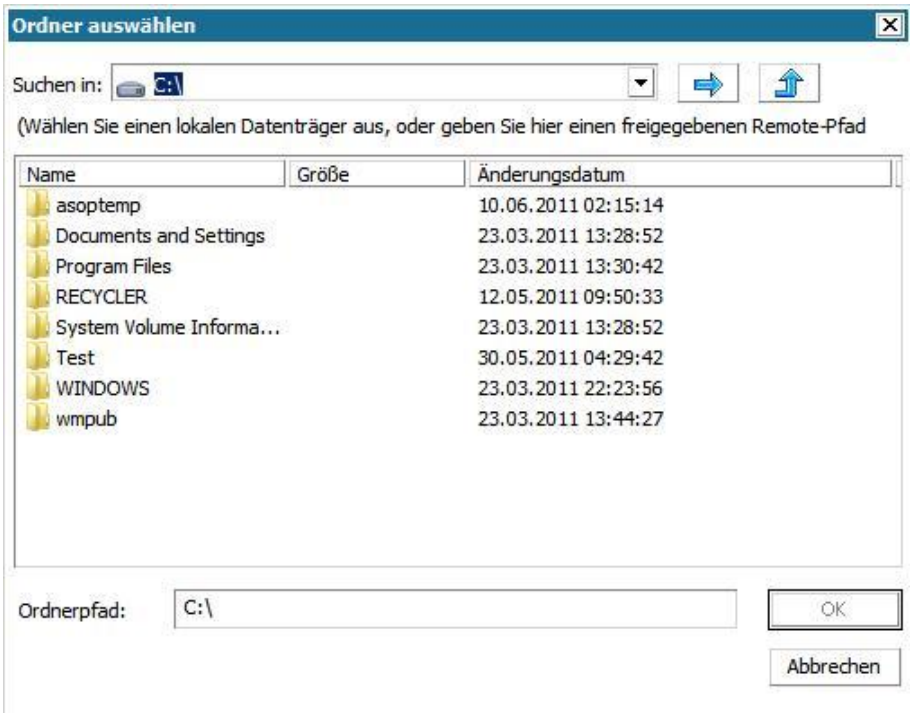
   Mit CA ARCserve D2D können Sie Wiederherstellungen von lokalen Laufwerken oder Netzwerkfreigaben durchführen.

   - Wenn Sie eine Wiederherstellung von einer lokalen Sicherung durchführen, erkennt der BMR-Assistent automatisch alle Volumes, die Wiederherstellungspunkte enthalten, und zeigt sie an.
   - Wenn Sie eine Wiederherstellung von einer Netzwerkfreigabe durchführen, müssen Sie den Remote-Speicherort der Wiederherstellungspunkte suchen. Wenn mehrere Rechner Wiederherstellungspunkte enthalten, werden sie alle angezeigt.

     Unter Umständen benötigen Sie Zugriffsinformationen (Benutzername und Kennwort) für den Remote-Rechner.

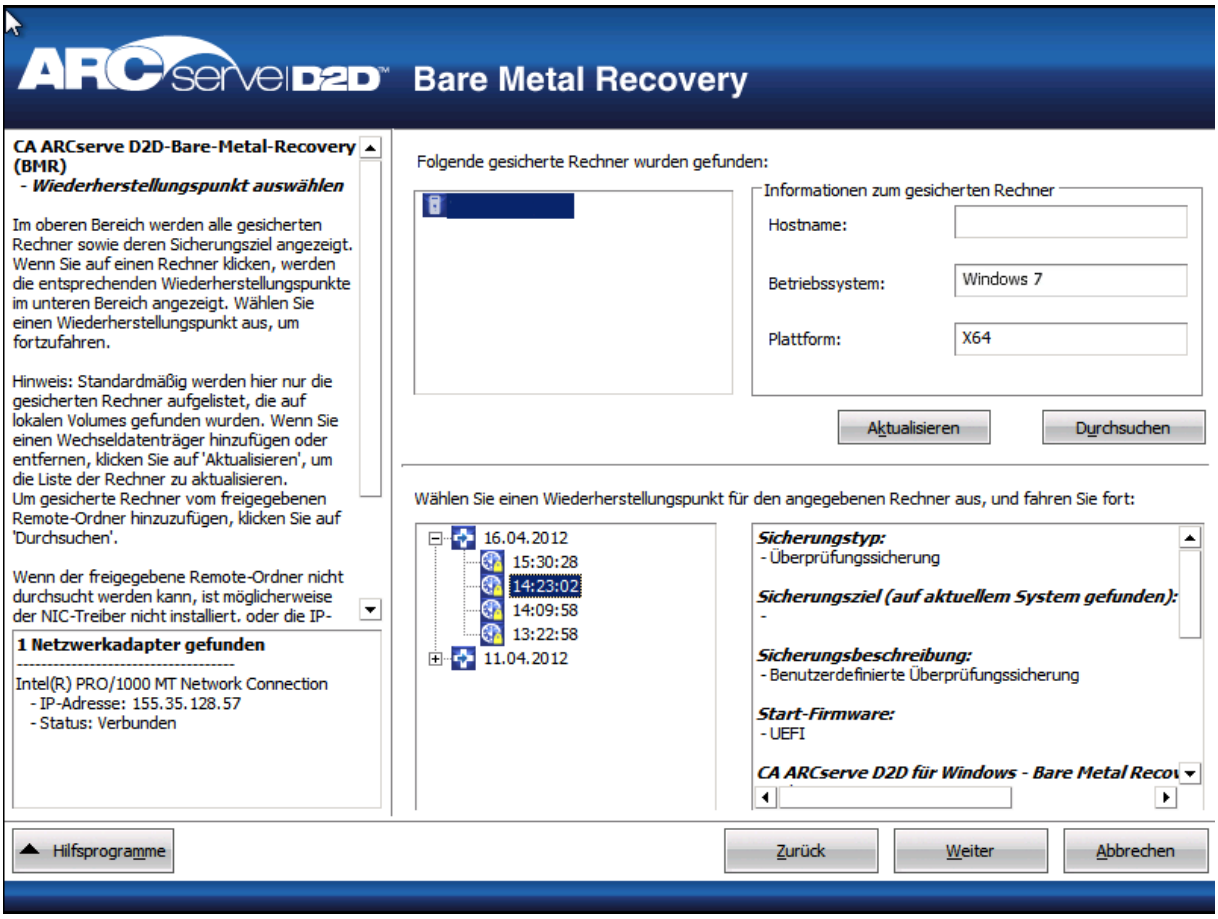
     Hinweis: Damit Sie das Netzwerk nach den Wiederherstellungspunkten durchsuchen können, muss die Netzwerkverbindung aktiv und verfügbar sein. Über das Menü "Hilfsprogramme" können Sie gegebenenfalls Ihre Netzwerkkonfigurationsinformationen überprüfen bzw. aktualisieren sowie fehlende Treiber laden.

6. Wenn das BMR-Modul kein lokales Zielvolume erkennt, wird automatisch das Dialogfeld "Ordner auswählen" angezeigt und Sie müssen angeben, wo die Sicherungen zu finden sind.



7. Wählen Sie den Ordner, in dem die Wiederherstellungspunkte für Ihre Sicherung gespeichert sind, und klicken Sie auf "OK". (Klicken Sie auf das Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen.)

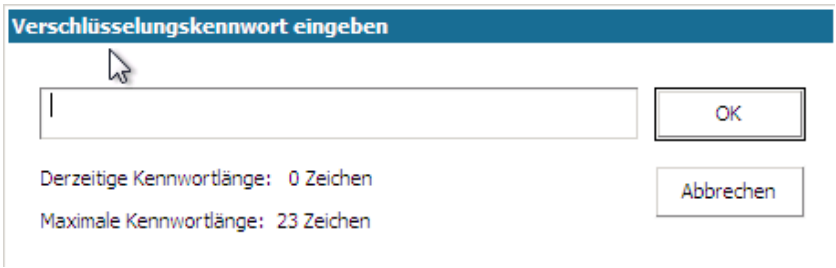
   Im BMR-Assistenten werden der Name des Rechners (im linken oberen Fensterbereich), mit ihm verbundene Sicherungsinformationen (im rechten oberen Fensterbereich) und alle dazugehörigen Wiederherstellungspunkte (im linken unteren Fensterbereich) angezeigt.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungspunkt auswählen
Im oberen Bereich werden alle gesicherten Rechner sowie deren Sicherungsziel angezeigt. Wenn Sie auf einen Rechner klicken, werden die entsprechenden Wiederherstellungspunkte im unteren Bereich angezeigt. Wählen Sie einen Wiederherstellungspunkt aus, um fortzufahren.
Hinweis: Standardmäßig werden hier nur die gesicherten Rechner aufgelistet, die auf lokalen Volumes gefunden wurden. Wenn Sie einen Wechseldatenträger hinzufügen oder entfernen, klicken Sie auf 'Aktualisieren', um die Liste der Rechner zu aktualisieren.
Um gesicherte Rechner vom freigegebenen Remote-Ordner hinzuzufügen, klicken Sie auf 'Durchsuchen'.
Wenn der freigegebene Remote-Ordner nicht durchsucht werden kann, ist möglicherweise der NIC-Treiber nicht installiert. oder die IP-
1 Netzwerkadapter gefunden
Intel(R) PRO/1000 MT Network Connection
- IP-Adresse: 155.35.128.57
- Status: Verbunden
Folgende gesicherte Rechner wurden gefunden:
Informationen zum gesicherten Rechner
Hostname:
Betriebssystem:
Windows 7
Plattform:
X64
Aktualisieren
Durchsuchen
Wählen Sie einen Wiederherstellungspunkt für den angegebenen Rechner aus, und fahren Sie fort:
16.04.2012
15:30:28
14:23:02
14:09:58
13:22:58
11.04.2012
Sicherungstyp:
- Überprüfungssicherung
Sicherungsziel (auf aktuellem System gefunden):
-
Sicherungsbeschreibung:
- Benutzerdefinierte Überprüfungssicherung
Start-Firmware:
- UEFI
CA ARCserve D2D für Windows - Bare Metal Recov
Hilfsprogramme
Zurück
Weiter
Abbrechen

8. Wählen Sie den wiederherzustellenden Wiederherstellungspunkt aus.

   Die Informationen zum ausgewählten Wiederherstellungspunkt werden angezeigt (im rechten unteren Fensterbereich). Diese Anzeige beinhaltet Informationen wie den Typ der durchgeführten (und gespeicherten) Sicherung, das Sicherungsziel und die gesicherten Volumes.

   Wenn der Wiederherstellungspunkt verschlüsselte Sitzungen enthält (das Uhrsymbol neben dem Wiederherstellungspunkt hat eine Sperre), wird ein Bildschirm zur Kennworteingabe geöffnet. Geben Sie das Sitzungskennwort ein, und klicken Sie auf "OK".



   Hinweis: Wenn es sich bei Ihrem Rechner um einen Domänen-Controller handelt, unterstützt CA ARCserve D2D eine nicht verbindliche Wiederherstellung der Active Directory (AD)-Datenbankdatei während einer Bare-Metal-Recovery. (Wiederherstellung von MSCS-Clustern ist nicht unterstützt.)

9. Überprüfen Sie, ob es sich um den gewünschten Wiederherstellungspunkt handelt, und klicken Sie auf "Weiter".

   Im BMR-Assistenten werden die verfügbaren Wiederherstellungsmodi angezeigt.

ARCserve D2D Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungsmodus auswählen
Welchen Wiederherstellungsmodus möchten Sie verwenden?
Express-Modus
Im Express-Modus wird das System automatisch durch nur minimales Eingreifen des Benutzers und die Verwendung der Standardeinstellungen des Rechners wiederhergestellt.
Erweiterter Modus
Der erweiterte Modus unterstützt Sie beim Anpassen des Wiederherstellungsprozesses. Mit diesem Modus können Sie folgende Aktionen ausführen:
Entscheiden, ob Sie Daten auf Basisvolumes oder dynamischen Volumes wiederherstellen möchten.
Gerätetreiber vor dem Neustart einfügen.
Hinweis: Wenn Sie auf 'Weiter' klicken, erstellt der BMR-Assistent neue Partitionen auf dem Zielrechner, die mit den Partitionen auf dem Quellrechner übereinstimmen. Möglicherweise werden Partitionen auf dem Zielrechner gelöscht und neue erstellt.
Hilfsprogramme
Zurück
Weiter
Abbrechen

10. Auswählen des Wiederherstellungsmodus

    Es stehen die Optionen "Erweiterter Modus" und "Express-Modus" zur Verfügung.

    - Wenn Sie den Wiederherstellungsprozess personalisieren möchten, wählen Sie "Erweiterter Modus".
    - Wenn Sie in den Wiederherstellungsprozess minimal eingreifen möchten, wählen Sie "Express-Modus".

    Standard: Express-Modus.

    Hinweis: Der restliche Vorgang gilt nur im erweiterten Modus, und der Vorgang enthält Informationen, die Sie durch die Bare-Metal-Recovery führen.

11. Klicken Sie auf "Weiter".

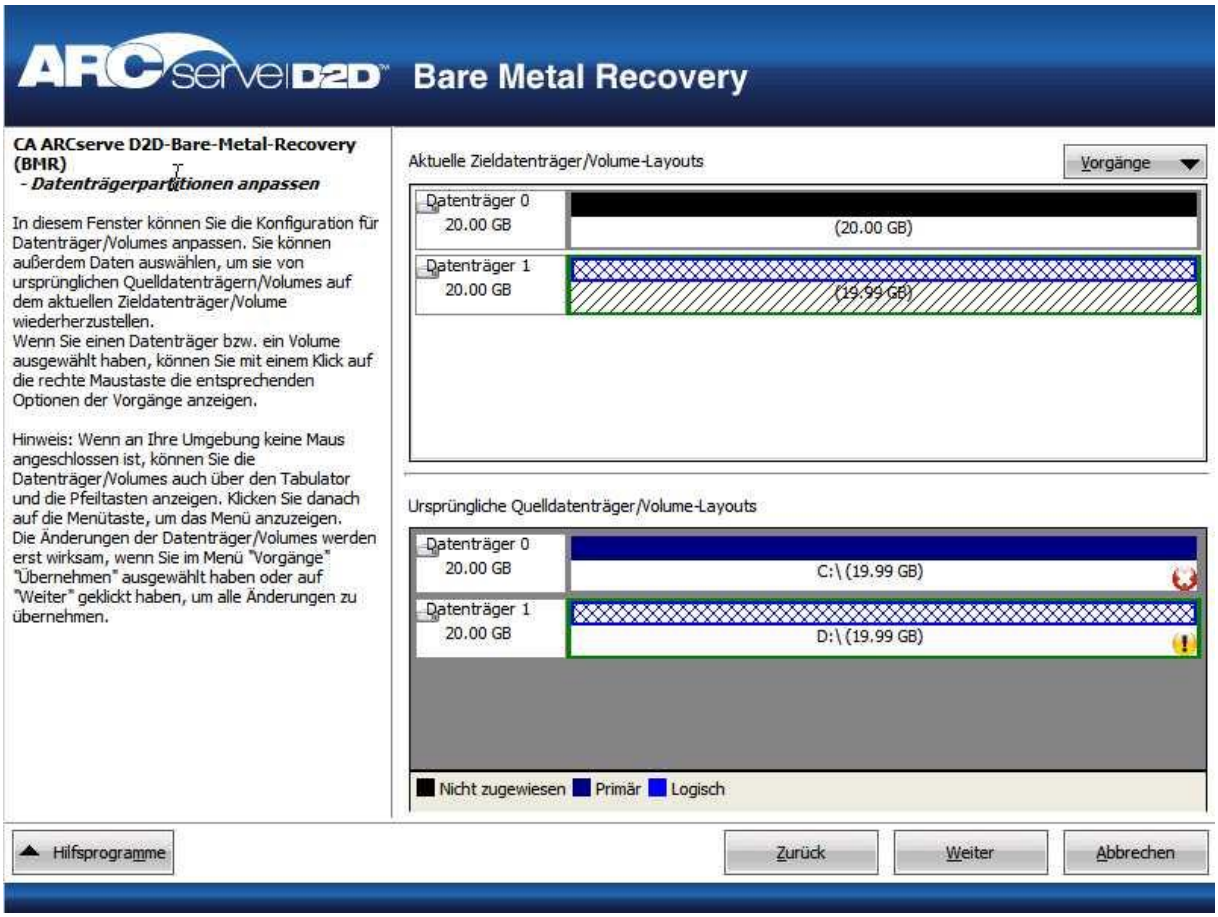
    Das BMR-Hilfsprogramm beginnt mit der Suche nach den wiederherzustellenden Rechnern und zeigt die entsprechenden Informationen zu Datenträgerpartitionen an.

    Im oberen Fensterbereich wird die Datenträgerkonfiguration des derzeitigen Rechners (Zielrechners) angezeigt. Im unteren Fensterbereich wird die Datenträgerkonfiguration angezeigt, die Sie am ursprünglichen Rechner (Quellrechner) eingestellt hatten.

Wichtig! Ein rotes X-Symbol, das für ein Quellvolume im unteren Bereich angezeigt wird, gibt an, dass dieses Volume Systeminformationen enthält und dem Zieldatenträger nicht zugewiesen (zugeordnet) wurde. Diese Systeminformationen müssen dem Zieldatenträger zugewiesen werden und während der Bare-Metal-Recovery wiederhergestellt werden. Anderenfalls schlägt der Neustart fehl.

Hinweis: Wenn Sie eine BMR ausführen und das Systemvolume auf einem Datenträger wiederherstellen, der nicht als Startdatenträger konfiguriert ist, kann der Rechner nicht gestartet werden, nachdem BMR abgeschlossen wurde. Stellen Sie sicher, dass Sie das Systemvolume auf einem ordnungsgemäß konfigurierten Startdatenträger wiederherstellen.

Hinweis: Bei einer Wiederherstellung auf einem anderen Datenträger oder Volume muss die Kapazität des neuen Datenträgers gleich oder größer als die des ursprünglichen Datenträgers/Volumes sein. Datenträger-Größenänderung ist außerdem nur bei Basisdatenträgern möglich, nicht bei dynamischen Datenträgern.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Datenträgerpartitionen anpassen
In diesem Fenster können Sie die Konfiguration für Datenträger/Volumes anpassen. Sie können außerdem Daten auswählen, um sie von ursprünglichen Quelldatenträgern/Volumes auf dem aktuellen Zieldatenträger/Volume wiederherzustellen.
Wenn Sie einen Datenträger bzw. ein Volume ausgewählt haben, können Sie mit einem Klick auf die rechte Maustaste die entsprechenden Optionen der Vorgänge anzeigen.
Hinweis: Wenn an Ihre Umgebung keine Maus angeschlossen ist, können Sie die Datenträger/Volumes auch über den Tabulator und die Pfeiltasten anzeigen. Klicken Sie danach auf die Menütaste, um das Menü anzuzeigen. Die Änderungen der Datenträger/Volumes werden erst wirksam, wenn Sie im Menü "Vorgänge" "Übernehmen" ausgewählt haben oder auf "Weiter" geklickt haben, um alle Änderungen zu übernehmen.
Aktuelle Zieldatenträger/Volume-Layouts
Vorgänge
Datenträger 0
20.00 GB
(20.00 GB)
Datenträger 1
20.00 GB
(19.99 GB)
Ursprüngliche Quelldatenträger/Volume-Layouts
Datenträger 0
20.00 GB
C:\ (19.99 GB)
Datenträger 1
20.00 GB
D:\ (19.99 GB)
Nicht zugewiesen
Primär
Logisch
Hilfsprogramme
Zurück
Weiter
Abbrechen

12. Wenn Ihnen die angezeigten aktuellen Datenträgerinformationen nicht richtig erscheinen, können Sie auf das Menü "Hilfsprogramm" zugreifen und nach eventuell fehlenden Treibern suchen.

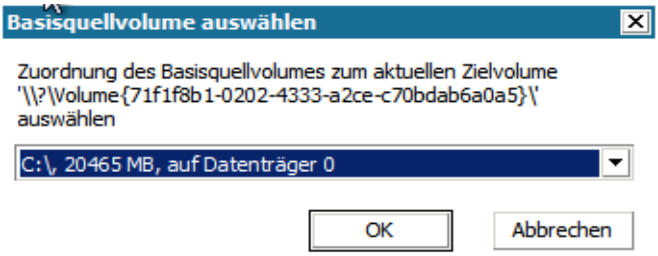
13. Wenn nötig, können Sie im Fensterbereich des Zielvolumes auf das Drop-down-Menü "Vorgänge" klicken, um die verfügbaren Optionen anzuzeigen.

    Von diesem Menü aus können Sie bestehende Partitionen zurücksetzen bzw. neue Partitionen erstellen, um den Datenträgerpartitionen auf dem Quellvolume zu entsprechen. (Zurücksetzen bedeutet, die Informationen zu Quell- und Zieldatenträgerlayout neu aus der Konfigurationsdatei und dem derzeitigen BS zu laden und alle vom Benutzer geänderten Informationen zum Datenträgerlayout zu verwerfen).

    Hinweis: Wenn Sie eine Zuordnung zu einem anderen Datenträger durchführen, muss die Kapazität jedes zugeordneten Zielvolume gleich oder größer als die des entsprechenden Quellvolumes sein.

14. Klicken Sie auf das entsprechende Zielvolume und wählen Sie im Popup-Menü die Option "Volume zuordnen von", um diesem Zielvolume ein Quellvolume zuzuordnen.

    Das Dialogfeld "Basisquellvolume auswählen" wird geöffnet.

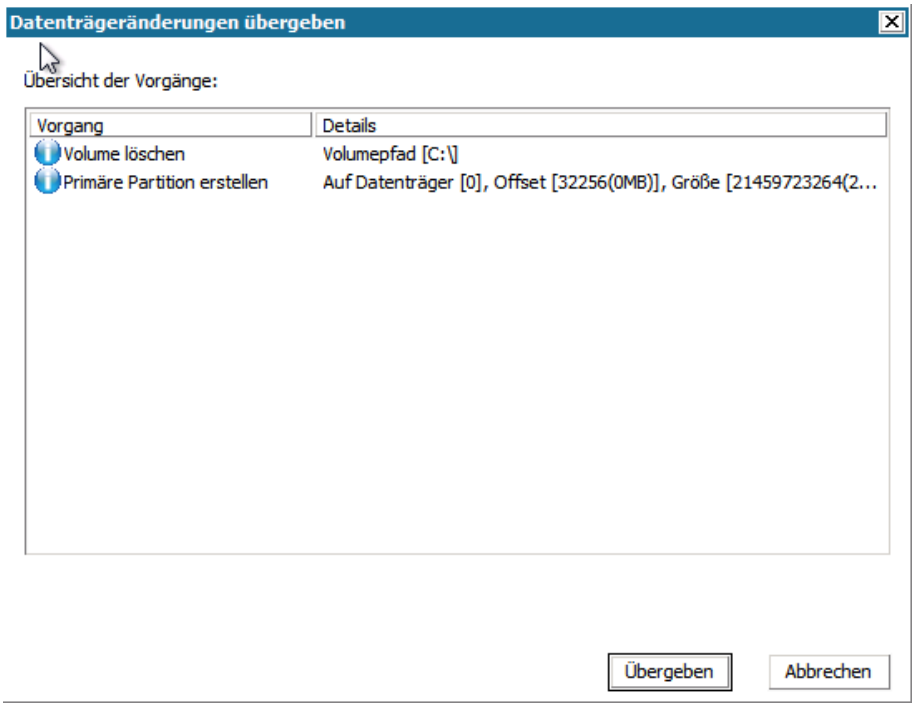


15. Klicken Sie im Dialogfeld "Basisquellvolume auswählen" auf das Drop-down-Menü, und wählen Sie das verfügbare Quellvolume, um es dem ausgewählten Zielvolume zuzuordnen. Klicken Sie auf "OK".

    - Im Zielvolume zeigt ein grünes hakenförmiges Symbol an, dass eine Zuordnung zu diesem Zielvolume durchgeführt wurde.
    - Im Quellvolume zeigt ein rotes x-förmiges Symbol an, dass dieses Quellvolume einem Zielvolume zugeordnet wurde.

16. Wenn Sie sicher sind, dass alle Volumes, die Sie wiederherstellen möchten, und alle Volumes, die Systeminformationen enthalten, einem Zielvolume zugeordnet sind, klicken Sie auf "Weiter".

    Im Bildschirm "Änderungen des Datenträgers übergeben" wird eine Übersicht über die ausgewählten Vorgänge angezeigt. Für jedes neu erstellte Volume werden die entsprechenden Informationen angezeigt.



17. Überprüfen Sie die Übersichtsinformationen, und klicken Sie auf "Übergeben". (Wenn die Informationen nicht richtig sind, klicken Sie auf "Abbrechen").

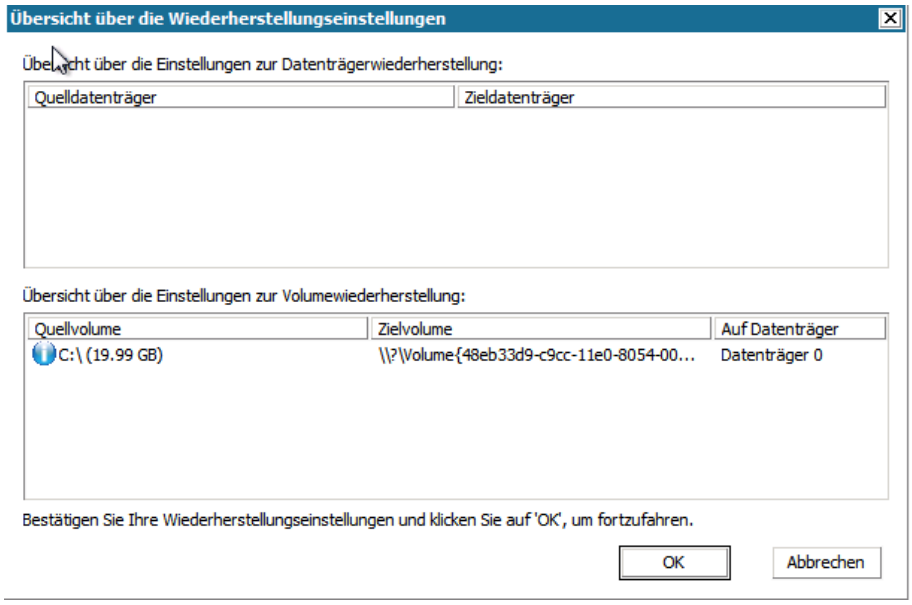
    Hinweis: Sämtliche Vorgänge, die die Festplatte betreffen, werden erst wirksam, wenn Sie sie übergeben haben.

    Auf dem Zielrechner werden die neuen Volumes erstellt und dem entsprechenden Quellrechner zugeordnet.

18. Wenn alle Änderungen abgeschlossen sind, klicken Sie auf "OK".

    Im Bildschirm "Übersicht über die Wiederherstellungseinstellungen" wird eine Übersicht der wiederherzustellenden Volumen angezeigt.

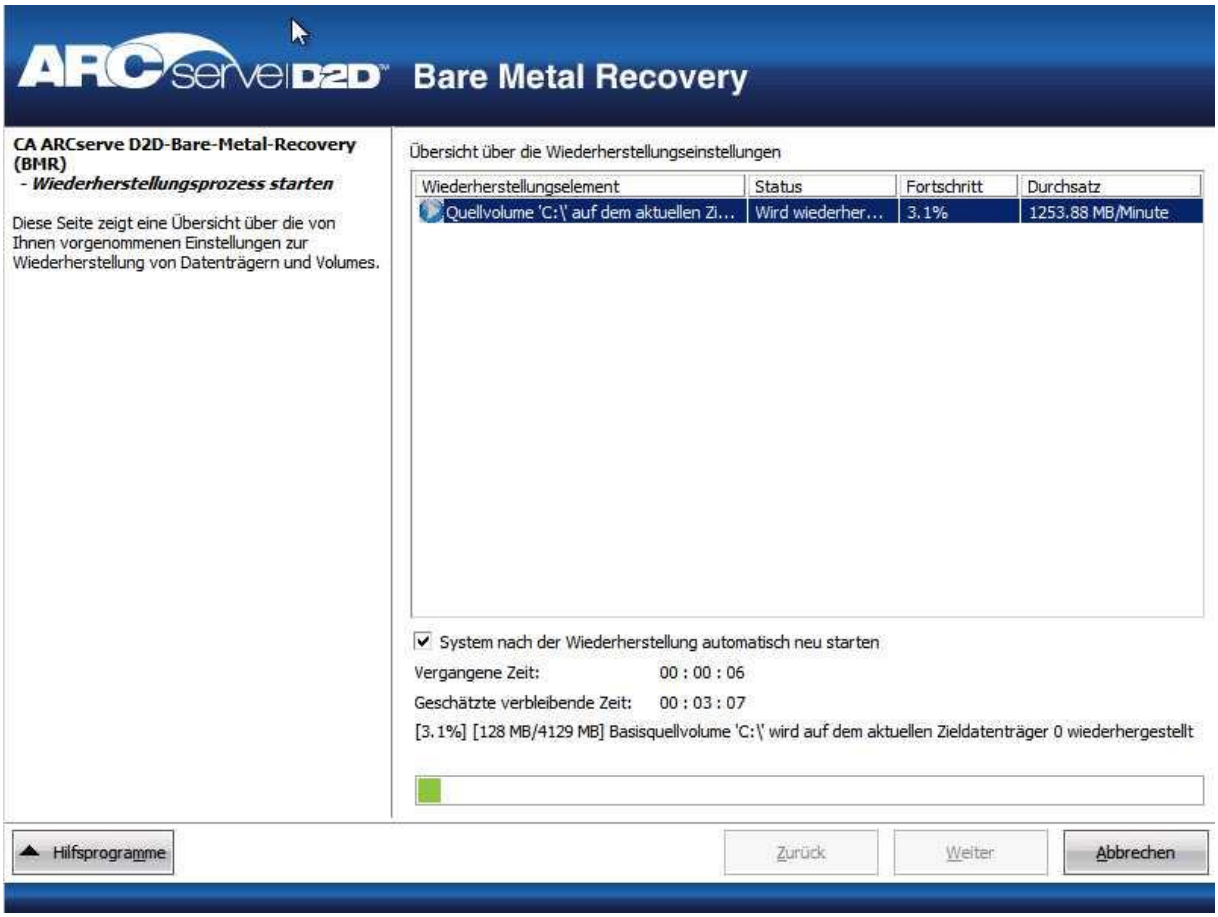
    Hinweis: Die Laufwerkbuchstaben, die unten in der Spalte "Zielvolume" aufgelistet werden, werden von Windows Preinstallation Environment (WinPE) automatisch erstellt. Sie können von den Laufwerkbuchstaben der Spalte "Quellvolume" abweichen. Auch wenn die Laufwerkbuchstaben nicht miteinander übereinstimmen werden die Daten im richtigen Volume ordnungsgemäß wiederhergestellt.



19. Nachdem Sie die Übersichtsinformationen überprüft haben, klicken Sie auf "OK".

    Der Wiederherstellungsprozess beginnt. Im BMR-Assistenten wird der Wiederherstellungsstatus jedes Volumes angezeigt.

    - Dieser Vorgang kann, abhängig von der Größe des Volumes, das wiederhergestellt wird, eine Weile dauern.
    - Sie stellen durch diesen Prozess sämtliche Informationen, die Sie für diesen Wiederherstellungspunkt gespeichert hatten, Block für Block wieder her und erstellen auf dem Zielrechner eine Kopie des Quellrechners.
    - Standardmäßig ist die Option, die nach der Wiederherstellung einen automatischen Systemneustart festlegt, aktiviert. Wenn nötig, können Sie diese Option löschen und den Neustart zu einem späteren Zeitpunkt manuell durchführen.
    - Sie können den Vorgang auch jederzeit abbrechen.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungsprozess starten
Diese Seite zeigt eine Übersicht über die von Ihnen vorgenommenen Einstellungen zur Wiederherstellung von Datenträgern und Volumes.
Übersicht über die Wiederherstellungseinstellungen
Wiederherstellungselement
Status
Fortschritt
Durchsatz
Quellvolume 'C:\' auf dem aktuellen Zi...
Wird wiederher...
3.1%
1253.88 MB/Minute
System nach der Wiederherstellung automatisch neu starten
Vergangene Zeit: 00 : 00 : 06
Geschätzte verbleibende Zeit: 00 : 03 : 07
[3.1%] [128 MB/4129 MB] Basisquellvolume 'C:\' wird auf dem aktuellen Zieldatenträger 0 wiederhergestellt
Hilfsprogramme
Zurück
Weiter
Abbrechen

20. Über das Hilfsprogramm-Menü können Sie auf das BMR-Aktivitätsprotokoll zugreifen und es mit der Option "Speichern" speichern.

    Der standardmäßige Speicherplatz für das Aktivitätsprotokoll ist folgender:

    X:\windows\system32\dr\log.

    Hinweis: Wenn Sie die Option "Speichern unter" des Fensters "BMR-Aktivitätsprotokoll" verwenden, sollten Sie, um Windows-bedingten Fehlern vorzubeugen, das Aktivitätsprotokoll nicht auf dem Desktop speichern oder einen Ordner auf dem Desktop dafür erstellen.

21. Wenn Sie die Wiederherstellung auf einer abweichenden Hardware durchführen (z. B. wenn der SCSI-/FC-Adapter, der zur Verbindung mit den Festplatten verwendet wurde, geändert wurde), und im ursprünglichen System kein kompatibler Treiber gefunden wird, wird die Seite "Treibereinfügung" angezeigt, über die Sie sich mit den benötigten Treibern versorgen können.

    Sie können das System durchsuchen und einzufügende Treiber auswählen, sodass sogar ein Rechner mit anderer Hardware nach einer Bare-Metal-Recovery wiederhergestellt werden kann.

22. Nach Abschluss der Bare-Metal-Recovery wird eine Bestätigungsmeldung angezeigt.

Hinweise: Nach Abschluss der BMR:

- Die erste Sicherung, die ausgeführt wird, ist eine Überprüfungssicherung.
- Wenn die Bare-Metal-Recovery abgeschlossen ist, sollten Sie überprüfen, ob das BIOS so konfiguriert ist, dass der Start vom Datenträger, auf dem das Boot-Volume wiederhergestellt wurde, durchgeführt wird.
- Wenn Sie auf abweichender Hardware wiederhergestellt haben, müssen Sie die Netzwerkadapter nach dem Neustart des Rechners möglicherweise manuell konfigurieren.
- Bei dynamischen Datenträgern können Sie den Offline-Status des Datenträgers über die Datenträgerverwaltung manuell in online umändern (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).
- Sie können dynamische Volumes auf dynamischen Datenträgern, die aufgrund von Redundanz fehlgeschlagen sind, über die Datenträgerverwaltung manuell neu synchronisieren (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).

Wiederherstellen von Quellservern mithilfe von Daten aus Hyper-V-basierten virtuellen Virtual Standby-Rechnern

Die Anwendung lässt Sie Quellserver mithilfe von CA ARCserve D2D-Daten wiederherstellen, die in Hyper-V-basierte virtuelle Virtual Standby-Rechner konvertiert wurden.

Hinweis: Die Anwendung verwendet den Bare-Metal-Recovery-Prozess, um Quellserver aus virtuellen Hyper-V-Rechnern wiederherzustellen. Weitere Informationen finden Sie unter Wiederherstellen von Quellservern mithilfe von Bare-Metal-Recovery (siehe Seite 122).

So stellen Sie Quellserver mithilfe von Daten aus Hyper-V-basierten virtuellen Virtual Standby-Rechnern wieder her

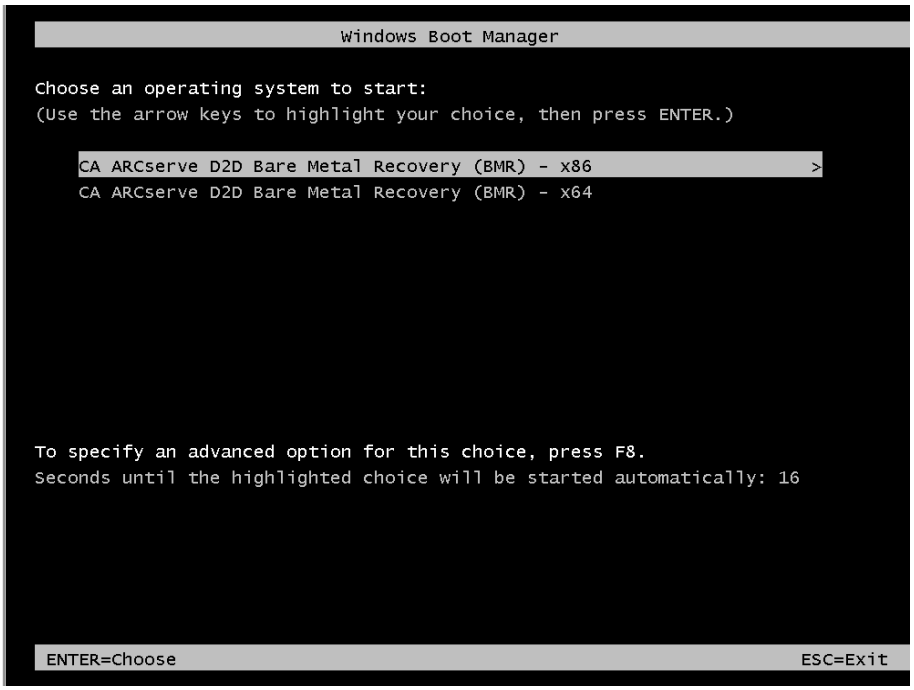
1. Legen Sie den Datenträger ein, auf dem das Bootkit-Image gespeichert ist, und starten Sie den Computer.

   - Wenn Sie ein abgespeichertes Windows Server PE-Image verwenden, legen Sie die entsprechende CD oder DVD ein.
   - Wenn Sie einen USB-Stick verwenden, legen Sie die Windows Server Installations-CD oder -DVD und anschließend den USB-Stick mit dem Bootkit-Image ein.

   Der Bildschirm des BIOS-Setup-Hilfsprogramms wird angezeigt.

2. Wählen Sie in diesem Bildschirm die Option "CD-ROM Drive", um den Neustart zu initiieren.

   Hinweis: Wenn Sie Windows PE-Image für BMR verwenden, müssen Sie eine Architektur (x86/x64) auswählen und auf "Eingabe" drücken, um fortzufahren.


Windows Boot Manager
Choose an operating system to start:
(Use the arrow keys to highlight your choice, then press ENTER.)
CA ARCserve D2D Bare Metal Recovery (BMR) - x86
CA ARCserve D2D Bare Metal Recovery (BMR) - x64
To specify an advanced option for this choice, press F8.
Seconds until the highlighted choice will be started automatically: 16
ENTER=Choose
ESC=Exit

3. Der CA ARCserve D2D-Bildschirm zur Sprachauswahl wird angezeigt. Wählen Sie eine Sprache aus und klicken Sie auf "Weiter", um fortzufahren.

   Hinweis: Wenn Sie BMR mit einem USB-Stick für BMR und einem Installationsdatenträger für
   Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 (CD/DVD)
   durchführen, der Multilingual User Interface (MUI) nicht unterstützt, wird der Bildschirm zur Sprachauswahl nicht angezeigt.

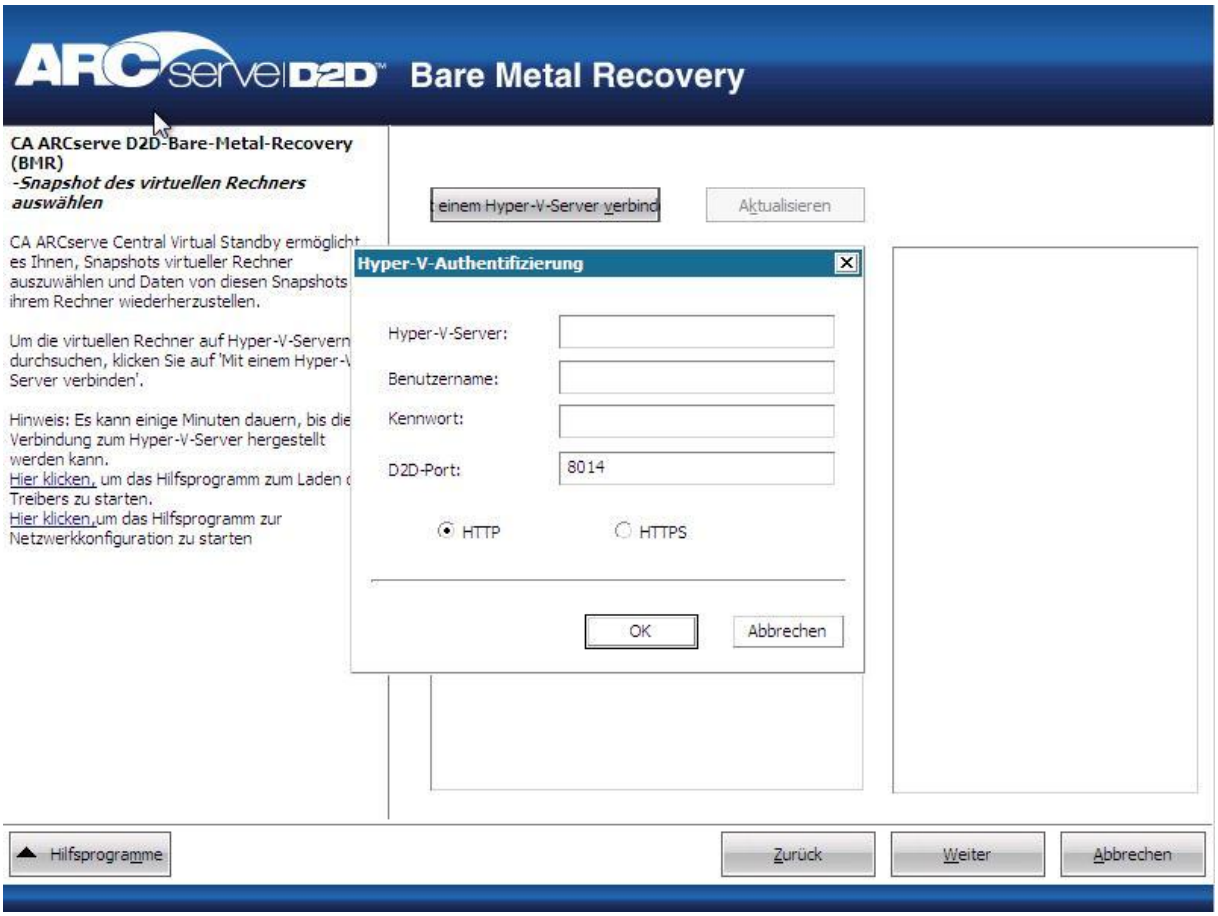
Die Bare-Metal-Recovery wird gestartet und der erste Bildschirm des BMR-Assistenten wird angezeigt.

4. Wählen Sie im Assistentenfenster für den Typ der Bare-Metal-Recovery (BMR) die Option "Wiederherstellen mit einer Hyper-V-Virtual Standby-VM" aus.

ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wählen Sie einen BMR-Typ aus
Legen Sie einen Wiederherstellungstyp fest:
Gesicherte Daten mit CA ARCserve D2D wiederherstellen
(Sicherungssitzungen mit CA ARCserve D2D oder CA ARCserve Central Host-Based VM Backup).
Wiederherstellen mit einer Hyper-V-Virtual Standby-VM
(Sie können Daten nur wiederherstellen, wenn die virtuelle Konvertierung mit CA ARCserve Central Virtual Standby ausgeführt wurde)
Wiederherstellen mit einer VMware-Virtual Standby-VM
(Sie können Daten nur wiederherstellen, wenn die virtuelle Konvertierung mit CA ARCserve Central Virtual Standby ausgeführt wurde)
Hilfsprogramme
Zurück
Weiter
Abbrechen

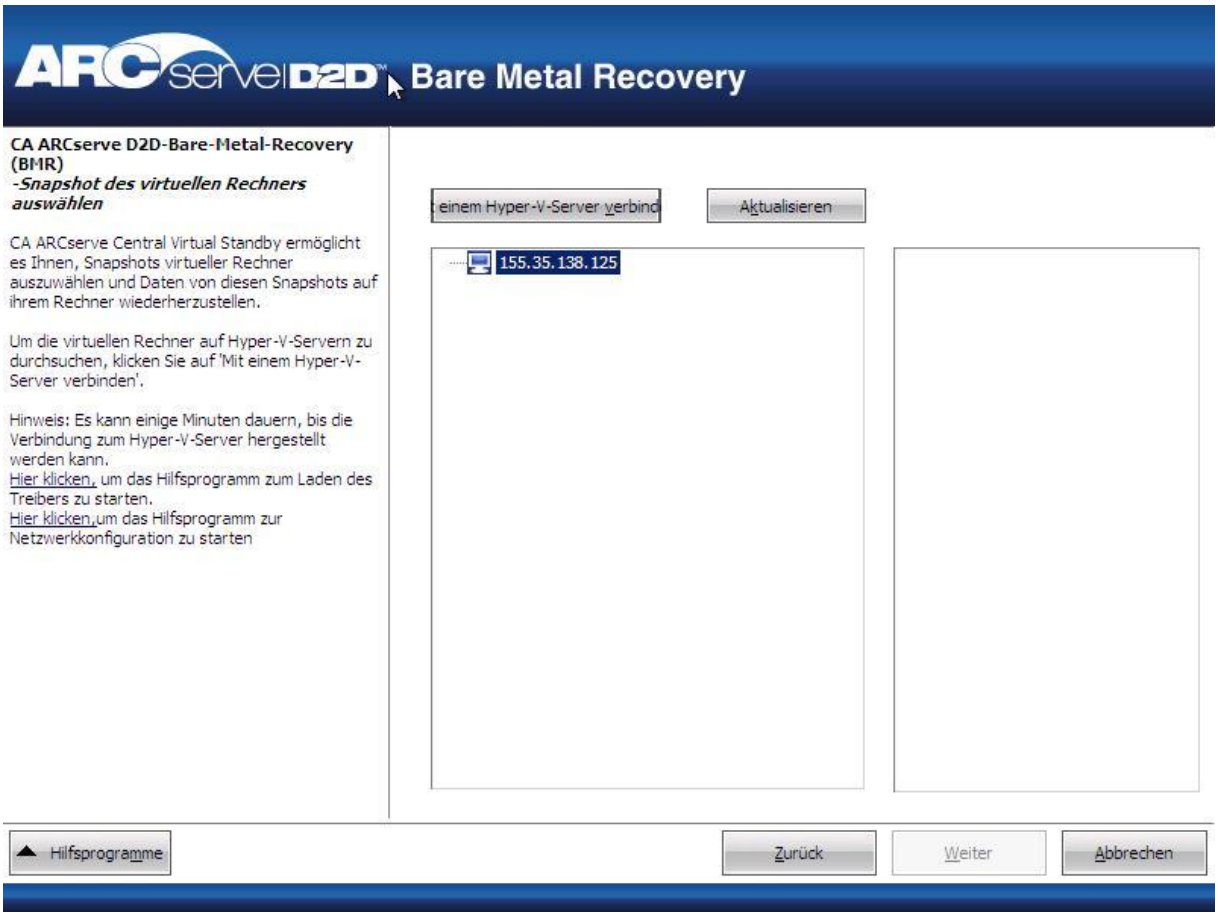
5. Klicken Sie auf "Weiter".

   Der Bildschirm "Snapshot des virtuellen Rechners auswählen" wird mit dem Dialogfeld "Hyper-V-Authentifizierung" angezeigt, und Sie werden aufgefordert, Hyper-V-Serverdetails einzugeben.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
-Snapshot des virtuellen Rechners auswählen
CA ARCserve Central Virtual Standby ermöglicht es Ihnen, Snapshots virtueller Rechner auszuwählen und Daten von diesen Snapshots ihrem Rechner wiederherzustellen.
Um die virtuellen Rechner auf Hyper-V-Servern durchsuchen, klicken Sie auf 'Mit einem Hyper-V Server verbinden'.
Hinweis: Es kann einige Minuten dauern, bis die Verbindung zum Hyper-V-Server hergestellt werden kann.
Hier klicken, um das Hilfsprogramm zum Laden Treibers zu starten.
Hier klicken, um das Hilfsprogramm zur Netzwerkkonfiguration zu starten
einem Hyper-V-Server verbind
Aktualisieren
Hyper-V-Authentifizierung
Hyper-V-Server:
Benutzername:
Kennwort:
D2D-Port:
8014
HTTP
HTTPS
OK
Abbrechen
Hilfsprogramme
Zurück
Weiter
Abbrechen

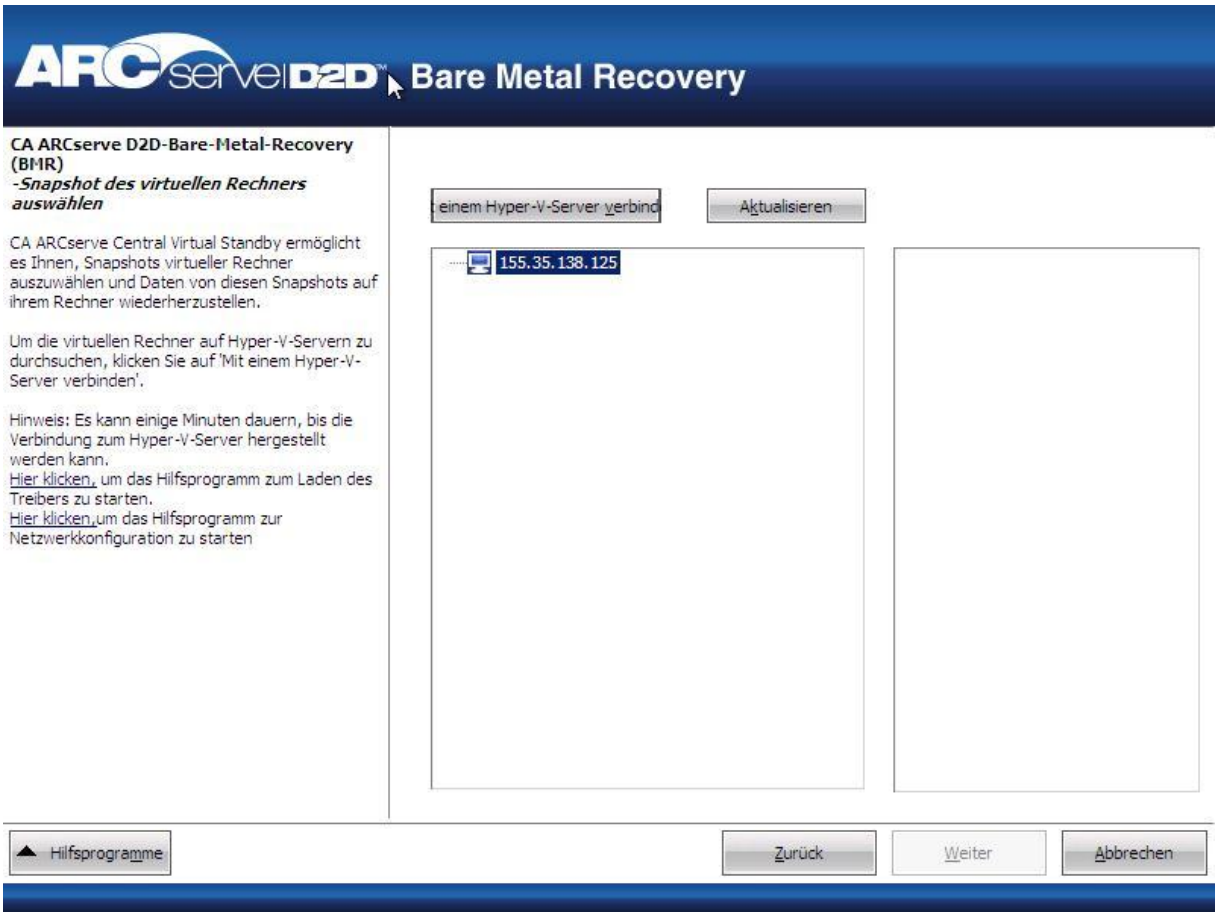
6. Geben Sie Authentifizierungsinformationen ein, und klicken Sie auf "OK".

   CA ARCserve D2D entdeckt und zeigt den Hyper-V-Server mit einer Auflistung aller virtuellen Rechner an, die in den angegebenen Hyper-V-Server mithilfe von CA ARCserve Central Virtual Standby konvertiert werden.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
-Snapshot des virtuellen Rechners auswählen
CA ARCserve Central Virtual Standby ermöglicht es Ihnen, Snapshots virtueller Rechner auszuwählen und Daten von diesen Snapshots auf ihrem Rechner wiederherzustellen.
Um die virtuellen Rechner auf Hyper-V-Servern zu durchsuchen, klicken Sie auf 'Mit einem Hyper-V-Server verbinden'.
Hinweis: Es kann einige Minuten dauern, bis die Verbindung zum Hyper-V-Server hergestellt werden kann.
Hier klicken, um das Hilfsprogramm zum Laden des Treibers zu starten.
Hier klicken,um das Hilfsprogramm zur Netzwerkkonfiguration zu starten
einem Hyper-V-Server verbind
Aktualisieren
155.35.138.125
Hilfsprogramme
Zurück
Weiter
Abbrechen

7. Wählen Sie den virtuellen Rechner aus, der Wiederherstellungspunkt-Snapshots für Ihr Sicherungs-Image enthält.

   Die Sicherungssitzungen (Wiederherstellungspunkt-Snapshots) für den ausgewählten virtuellen Rechner werden angezeigt.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
-Snapshot des virtuellen Rechners auswählen
CA ARCserve Central Virtual Standby ermöglicht es Ihnen, Snapshots virtueller Rechner auszuwählen und Daten von diesen Snapshots auf ihrem Rechner wiederherzustellen.
Um die virtuellen Rechner auf Hyper-V-Servern zu durchsuchen, klicken Sie auf 'Mit einem Hyper-V-Server verbinden'.
Hinweis: Es kann einige Minuten dauern, bis die Verbindung zum Hyper-V-Server hergestellt werden kann.
Hier klicken, um das Hilfsprogramm zum Laden des Treibers zu starten.
Hier klicken,um das Hilfsprogramm zur Netzwerkkonfiguration zu starten
einem Hyper-V-Server verbind
Aktualisieren
155.35.138.125
Hilfsprogramme
Zurück
Weiter
Abbrechen

8. Wählen Sie die Sicherungssitzung des virtuellen Rechners (Wiederherstellungspunkt-Snapshot), die Sie wiederherstellen möchten.

   Die entsprechenden Details für den ausgewählten Wiederherstellungspunkt-Snapshot (Name des virtuellen Rechners, Name der Sicherungssitzung, gesicherte Volumes) werden im rechten Bereich angezeigt.

   Sie können einen der aufgelisteten Wiederherstellungspunkte auswählen und haben dazu noch die Möglichkeit, den Wiederherstellungspunkt "Aktueller Status" oder "Letzter Status" auszuwählen.

   - Wenn der virtuelle Rechner, von dem Sie eine Wiederherstellung durchführen, aktiviert ist, wird der Wiederherstellungspunkt "Aktueller Status" angezeigt.
   - Wenn der virtuelle Rechner, von dem Sie eine Wiederherstellung durchführen, deaktiviert ist, wird der Wiederherstellungspunkt "Letzter Status" angezeigt.

     Wenn Sie den Wiederherstellungspunkt "Letzter Status" auswählen, wird eine Fehlermeldung angezeigt, um Sie darüber zu informieren, dass der Wiederherstellungspunkt, von dem Sie eine Wiederherstellung durchführen, der Status "Letzter Status" (und nicht "Aktueller Status") ist. Es wird verlangt, dass Sie den virtuellen Rechner starten, bevor Sie mit der Wiederherstellung fortfahren.

9. Überprüfen Sie, ob es sich um den gewünschten Wiederherstellungspunkt handelt, und klicken Sie auf "Weiter".

   Im BMR-Assistenten werden die verfügbaren Wiederherstellungsmodi angezeigt.

10. Auswählen des Wiederherstellungsmodus

    Es stehen die Optionen "Erweiterter Modus" und "Express-Modus" zur Verfügung.

    - Wenn Sie den Wiederherstellungsprozess personalisieren möchten, wählen Sie "Erweiterter Modus".
    - Wenn Sie in den Wiederherstellungsprozess minimal eingreifen möchten, wählen Sie "Express-Modus".

    Standard: Express-Modus.

    Hinweis: Der restliche Vorgang gilt nur im erweiterten Modus, und der Vorgang enthält Informationen, die Sie durch die Bare-Metal-Recovery führen.

11. Klicken Sie auf "Weiter".

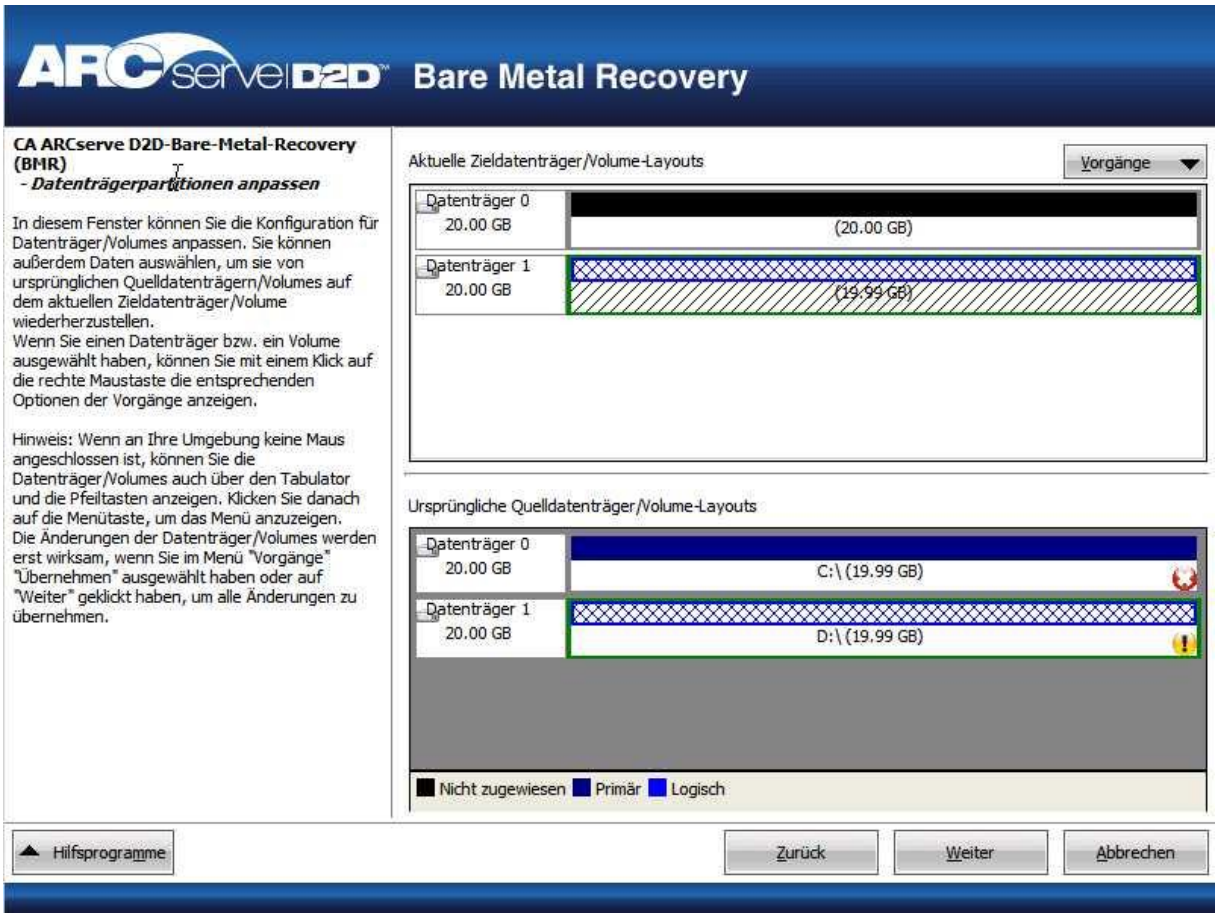
    Das BMR-Hilfsprogramm beginnt mit der Suche nach den wiederherzustellenden Rechnern und zeigt die entsprechenden Informationen zu Datenträgerpartitionen an.

    Im oberen Fensterbereich wird die Datenträgerkonfiguration des derzeitigen Rechners (Zielrechners) angezeigt. Im unteren Fensterbereich wird die Datenträgerkonfiguration angezeigt, die Sie am ursprünglichen Rechner (Quellrechner) eingestellt hatten.

Wichtig! Ein rotes X-Symbol, das für ein Quellvolume im unteren Bereich angezeigt wird, gibt an, dass dieses Volume Systeminformationen enthält und dem Zieldatenträger nicht zugewiesen (zugeordnet) wurde. Diese Systeminformationen müssen dem Zieldatenträger zugewiesen werden und während der Bare-Metal-Recovery wiederhergestellt werden. Anderenfalls schlägt der Neustart fehl.

Hinweis: Wenn Sie eine BMR ausführen und das Systemvolume auf einem Datenträger wiederherstellen, der nicht als Startdatenträger konfiguriert ist, kann der Rechner nicht gestartet werden, nachdem BMR abgeschlossen wurde. Stellen Sie sicher, dass Sie das Systemvolume auf einem ordnungsgemäß konfigurierten Startdatenträger wiederherstellen.

Hinweis: Bei einer Wiederherstellung auf einem anderen Datenträger oder Volume muss die Kapazität des neuen Datenträgers gleich oder größer als die des ursprünglichen Datenträgers/Volumes sein. Datenträger-Größenänderung ist außerdem nur bei Basisdatenträgern möglich, nicht bei dynamischen Datenträgern.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Datenträgerpartitionen anpassen
In diesem Fenster können Sie die Konfiguration für Datenträger/Volumes anpassen. Sie können außerdem Daten auswählen, um sie von ursprünglichen Quelldatenträgern/Volumes auf dem aktuellen Zieldatenträger/Volume wiederherzustellen.
Wenn Sie einen Datenträger bzw. ein Volume ausgewählt haben, können Sie mit einem Klick auf die rechte Maustaste die entsprechenden Optionen der Vorgänge anzeigen.
Hinweis: Wenn an Ihre Umgebung keine Maus angeschlossen ist, können Sie die Datenträger/Volumes auch über den Tabulator und die Pfeiltasten anzeigen. Klicken Sie danach auf die Menütaste, um das Menü anzuzeigen. Die Änderungen der Datenträger/Volumes werden erst wirksam, wenn Sie im Menü "Vorgänge" "Übernehmen" ausgewählt haben oder auf "Weiter" geklickt haben, um alle Änderungen zu übernehmen.
Aktuelle Zieldatenträger/Volume-Layouts
Vorgänge
Datenträger 0
20.00 GB
(20.00 GB)
Datenträger 1
20.00 GB
(19.99 GB)
Ursprüngliche Quelldatenträger/Volume-Layouts
Datenträger 0
20.00 GB
C:\ (19.99 GB)
Datenträger 1
20.00 GB
D:\ (19.99 GB)
Nicht zugewiesen
Primär
Logisch
Hilfsprogramme
Zurück
Weiter
Abbrechen

12. Wenn Ihnen die angezeigten aktuellen Datenträgerinformationen nicht richtig erscheinen, können Sie auf das Menü "Hilfsprogramm" zugreifen und nach eventuell fehlenden Treibern suchen.

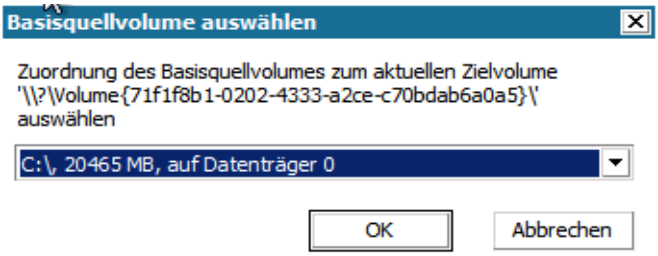
13. Wenn nötig, können Sie im Fensterbereich des Zielvolumes auf das Drop-down-Menü "Vorgänge" klicken, um die verfügbaren Optionen anzuzeigen.

    Von diesem Menü aus können Sie bestehende Partitionen zurücksetzen bzw. neue Partitionen erstellen, um den Datenträgerpartitionen auf dem Quellvolume zu entsprechen. (Zurücksetzen bedeutet, die Informationen zu Quell- und Zieldatenträgerlayout neu aus der Konfigurationsdatei und dem derzeitigen BS zu laden und alle vom Benutzer geänderten Informationen zum Datenträgerlayout zu verwerfen).

    Hinweis: Wenn Sie eine Zuordnung zu einem anderen Datenträger durchführen, muss die Kapazität jedes zugeordneten Zielvolume gleich oder größer als die des entsprechenden Quellvolumes sein.

14. Klicken Sie auf das entsprechende Zielvolume und wählen Sie im Popup-Menü die Option "Volume zuordnen von", um diesem Zielvolume ein Quellvolume zuzuordnen.

    Das Dialogfeld "Basisquellvolume auswählen" wird geöffnet.

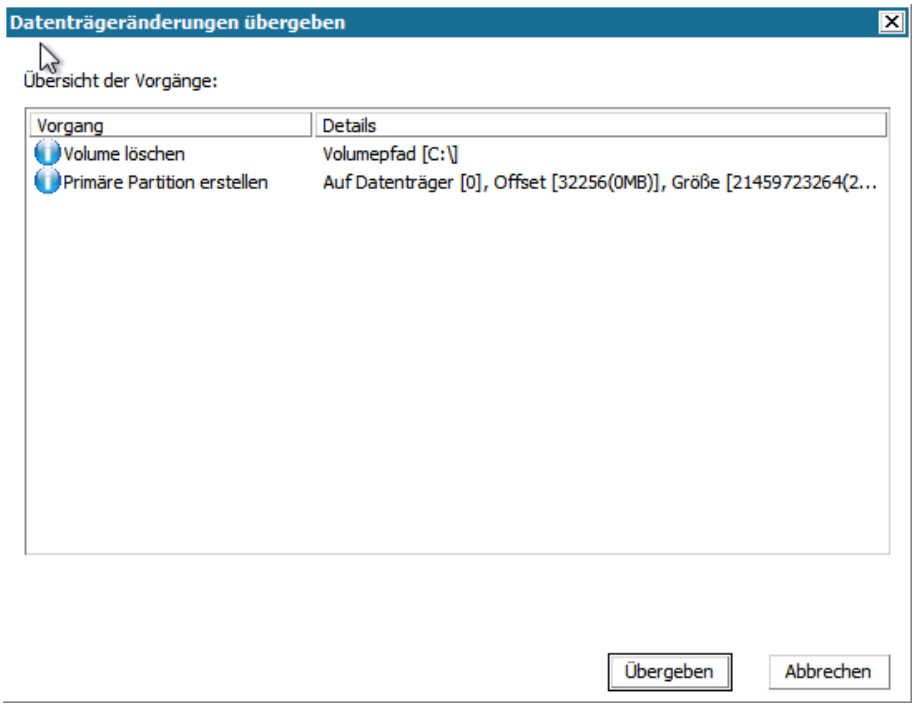


15. Klicken Sie im Dialogfeld "Basisquellvolume auswählen" auf das Drop-down-Menü, und wählen Sie das verfügbare Quellvolume, um es dem ausgewählten Zielvolume zuzuordnen. Klicken Sie auf "OK".

    - Im Zielvolume zeigt ein grünes hakenförmiges Symbol an, dass eine Zuordnung zu diesem Zielvolume durchgeführt wurde.
    - Im Quellvolume zeigt ein rotes x-förmiges Symbol an, dass dieses Quellvolume einem Zielvolume zugeordnet wurde.

16. Wenn Sie sicher sind, dass alle Volumes, die Sie wiederherstellen möchten, und alle Volumes, die Systeminformationen enthalten, einem Zielvolume zugeordnet sind, klicken Sie auf "Weiter".

    Im Bildschirm "Änderungen des Datenträgers übergeben" wird eine Übersicht über die ausgewählten Vorgänge angezeigt. Für jedes neu erstellte Volume werden die entsprechenden Informationen angezeigt.



17. Überprüfen Sie die Übersichtsinformationen, und klicken Sie auf "Übergeben". (Wenn die Informationen nicht richtig sind, klicken Sie auf "Abbrechen").

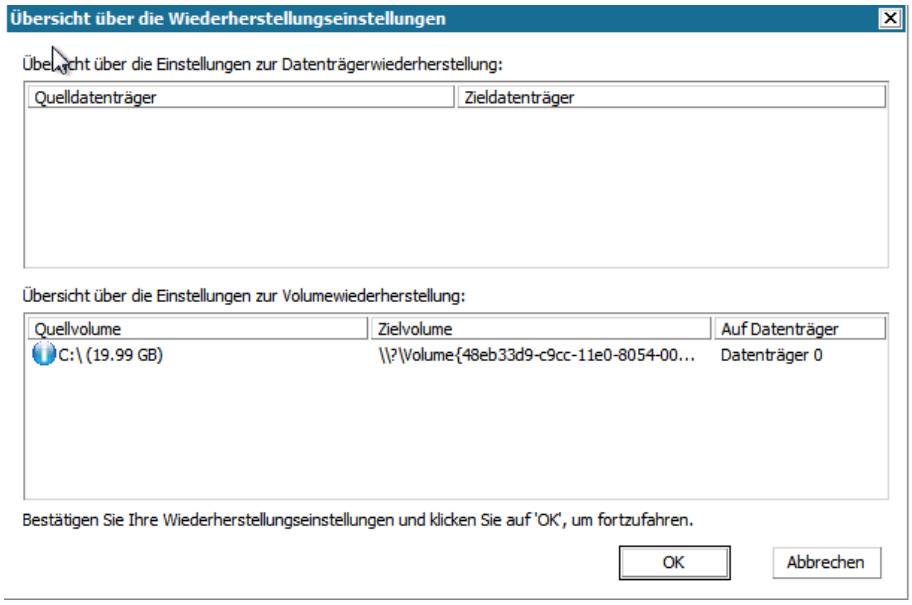
    Hinweis: Sämtliche Vorgänge, die die Festplatte betreffen, werden erst wirksam, wenn Sie sie übergeben haben.

    Auf dem Zielrechner werden die neuen Volumes erstellt und dem entsprechenden Quellrechner zugeordnet.

18. Wenn alle Änderungen abgeschlossen sind, klicken Sie auf "OK".

    Im Bildschirm "Übersicht über die Wiederherstellungseinstellungen" wird eine Übersicht der wiederherzustellenden Volumen angezeigt.

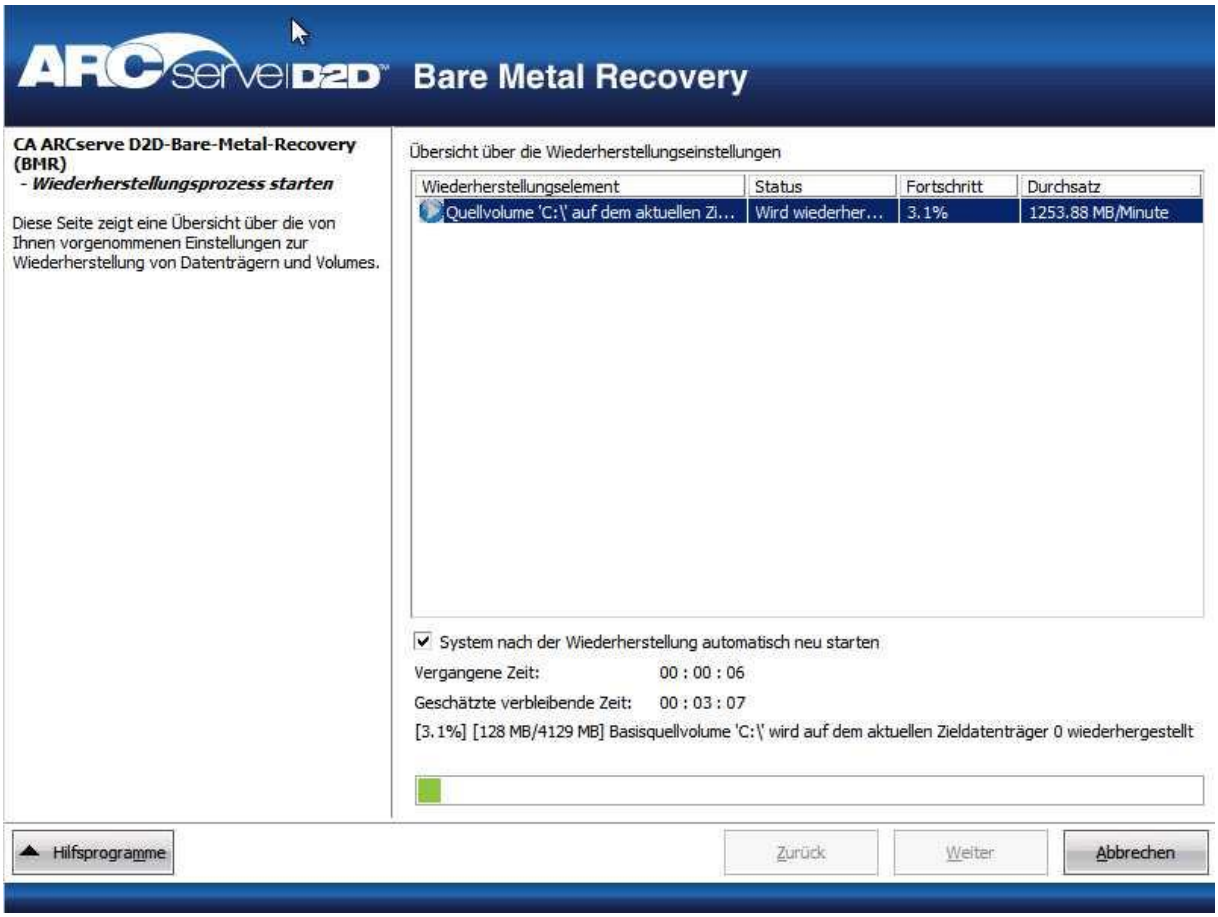
    Hinweis: Die Laufwerkbuchstaben, die unten in der Spalte "Zielvolume" aufgelistet werden, werden von Windows Preinstallation Environment (WinPE) automatisch erstellt. Sie können von den Laufwerkbuchstaben der Spalte "Quellvolume" abweichen. Auch wenn die Laufwerkbuchstaben nicht miteinander übereinstimmen werden die Daten im richtigen Volume ordnungsgemäß wiederhergestellt.



19. Nachdem Sie die Übersichtsinformationen überprüft haben, klicken Sie auf "OK".

    Der Wiederherstellungsprozess beginnt. Im BMR-Assistenten wird der Wiederherstellungsstatus jedes Volumes angezeigt.

    - Dieser Vorgang kann, abhängig von der Größe des Volumes, das wiederhergestellt wird, eine Weile dauern.
    - Sie stellen durch diesen Prozess sämtliche Informationen, die Sie für diesen Wiederherstellungspunkt gespeichert hatten, Block für Block wieder her und erstellen auf dem Zielrechner eine Kopie des Quellrechners.
    - Standardmäßig ist die Option, die nach der Wiederherstellung einen automatischen Systemneustart festlegt, aktiviert. Wenn nötig, können Sie diese Option löschen und den Neustart zu einem späteren Zeitpunkt manuell durchführen.
    - Sie können den Vorgang auch jederzeit abbrechen.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungsprozess starten
Diese Seite zeigt eine Übersicht über die von Ihnen vorgenommenen Einstellungen zur Wiederherstellung von Datenträgern und Volumes.
Übersicht über die Wiederherstellungseinstellungen
Wiederherstellungselement
Status
Fortschritt
Durchsatz
Quellvolume 'C:\' auf dem aktuellen Zi...
Wird wiederher...
3.1%
1253.88 MB/Minute
System nach der Wiederherstellung automatisch neu starten
Vergangene Zeit: 00 : 00 : 06
Geschätzte verbleibende Zeit: 00 : 03 : 07
[3.1%] [128 MB/4129 MB] Basisquellvolume 'C:\' wird auf dem aktuellen Zieldatenträger 0 wiederhergestellt
Hilfsprogramme
Zurück
Weiter
Abbrechen

20. Über das Hilfsprogramm-Menü können Sie auf das BMR-Aktivitätsprotokoll zugreifen und es mit der Option "Speichern" speichern.

    Der standardmäßige Speicherplatz für das Aktivitätsprotokoll ist folgender:

    X:\windows\system32\dr\log.

    Hinweis: Wenn Sie die Option "Speichern unter" des Fensters "BMR-Aktivitätsprotokoll" verwenden, sollten Sie, um Windows-bedingten Fehlern vorzubeugen, das Aktivitätsprotokoll nicht auf dem Desktop speichern oder einen Ordner auf dem Desktop dafür erstellen.

21. Wenn Sie die Wiederherstellung auf einer abweichenden Hardware durchführen (z. B. wenn der SCSI-/FC-Adapter, der zur Verbindung mit den Festplatten verwendet wurde, geändert wurde), und im ursprünglichen System kein kompatibler Treiber gefunden wird, wird die Seite "Treibereinfügung" angezeigt, über die Sie sich mit den benötigten Treibern versorgen können.

    Sie können das System durchsuchen und einzufügende Treiber auswählen, sodass sogar ein Rechner mit anderer Hardware nach einer Bare-Metal-Recovery wiederhergestellt werden kann.

22. Nach Abschluss der Bare-Metal-Recovery wird eine Bestätigungsmeldung angezeigt.

Hinweise: Nach Abschluss der BMR:

- Die erste Sicherung, die ausgeführt wird, ist eine Überprüfungssicherung.
- Wenn die Bare-Metal-Recovery abgeschlossen ist, sollten Sie überprüfen, ob das BIOS so konfiguriert ist, dass der Start vom Datenträger, auf dem das Boot-Volume wiederhergestellt wurde, durchgeführt wird.
- Wenn Sie auf abweichender Hardware wiederhergestellt haben, müssen Sie die Netzwerkadapter nach dem Neustart des Rechners möglicherweise manuell konfigurieren.
- Bei dynamischen Datenträgern können Sie den Offline-Status des Datenträgers über die Datenträgerverwaltung manuell in online umändern (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).
- Sie können dynamische Volumes auf dynamischen Datenträgern, die aufgrund von Redundanz fehlgeschlagen sind, über die Datenträgerverwaltung manuell neu synchronisieren (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).

Wiederherstellen von Quellservern mithilfe von Daten aus VMware-basierten virtuellen Virtual Standby-Rechnern

Die Anwendung lässt Sie Quellserver mithilfe von CA ARCserve D2D-Daten wiederherstellen, die in VMware-basierte virtuelle Virtual Standby-Rechner konvertiert wurden.

Hinweis: Die Anwendung verwendet den Bare-Metal-Recovery-Prozess, um Quellserver aus virtuellen VMware-Rechnern wiederherzustellen. Weitere Informationen finden Sie unter Wiederherstellen von Quellservern mithilfe von Bare-Metal-Recovery (siehe Seite 122).

So stellen Sie Quellserver mithilfe von Daten aus VMware-basierten virtuellen Virtual Standby-Rechnern wieder her

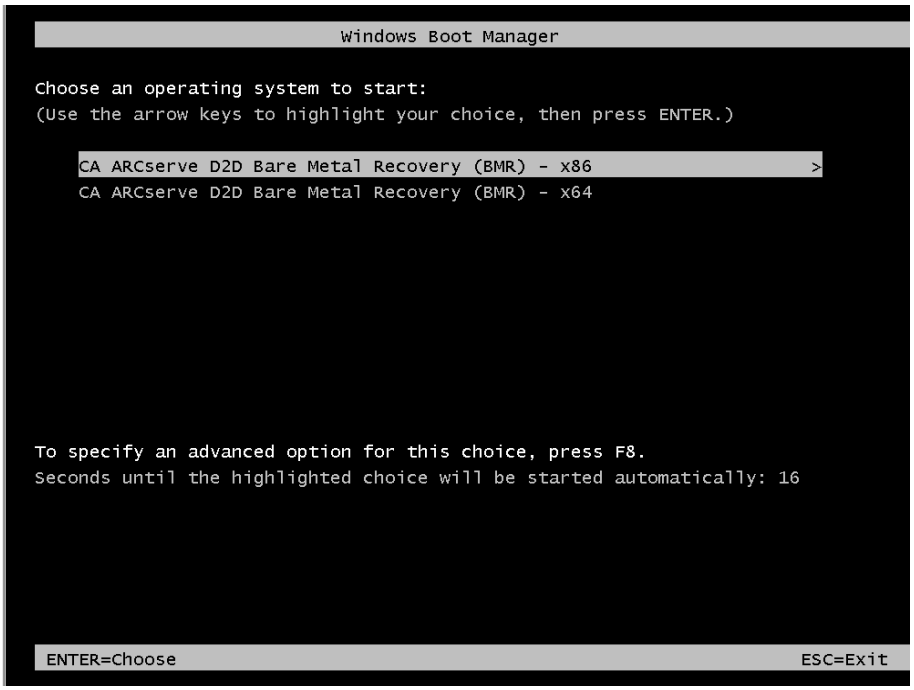
1. Legen Sie den Datenträger ein, auf dem das Bootkit-Image gespeichert ist, und starten Sie den Computer.

   - Wenn Sie ein abgespeichertes Windows Server PE-Image verwenden, legen Sie die entsprechende CD oder DVD ein.
   - Wenn Sie einen USB-Stick verwenden, legen Sie die Windows Server Installations-CD oder -DVD und anschließend den USB-Stick mit dem Bootkit-Image ein.

   Der Bildschirm des BIOS-Setup-Hilfsprogramms wird angezeigt.

2. Wählen Sie in diesem Bildschirm die Option "CD-ROM Drive", um den Neustart zu initiieren.

   Hinweis: Wenn Sie Windows PE-Image für BMR verwenden, müssen Sie eine Architektur (x86/x64) auswählen und auf "Eingabe" drücken, um fortzufahren.


Windows Boot Manager
Choose an operating system to start:
(Use the arrow keys to highlight your choice, then press ENTER.)
CA ARCserve D2D Bare Metal Recovery (BMR) - x86
CA ARCserve D2D Bare Metal Recovery (BMR) - x64
To specify an advanced option for this choice, press F8.
Seconds until the highlighted choice will be started automatically: 16
ENTER=Choose
ESC=Exit

3. Der CA ARCserve D2D-Bildschirm zur Sprachauswahl wird angezeigt. Wählen Sie eine Sprache aus und klicken Sie auf "Weiter", um fortzufahren.

   Hinweis: Wenn Sie BMR mit einem USB-Stick für BMR und einem Installationsdatenträger für
   Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 (CD/DVD)
   durchführen, der Multilingual User Interface (MUI) nicht unterstützt, wird der Bildschirm zur Sprachauswahl nicht angezeigt.

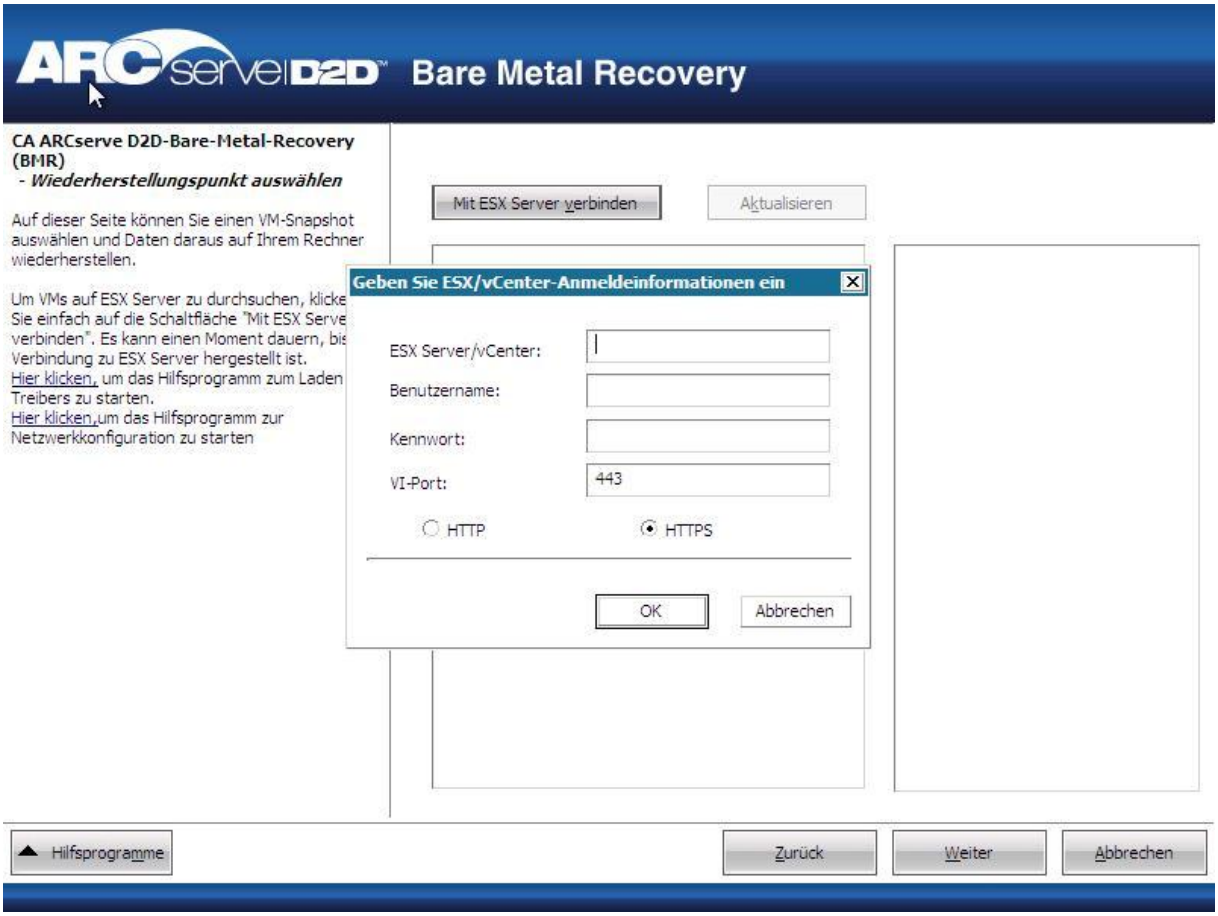
Die Bare-Metal-Recovery wird gestartet und der erste Bildschirm des BMR-Assistenten wird angezeigt.

4. Wählen Sie im Assistentenfenster für den Typ der Bare-Metal-Recovery (BMR) die Option "Wiederherstellen mit einer VMware-Virtual Standby-VM" aus.

ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wählen Sie einen BMR-Typ aus
Legen Sie einen Wiederherstellungstyp fest:
Gesicherte Daten mit CA ARCserve D2D wiederherstellen
(Sicherungssitzungen mit CA ARCserve D2D oder CA ARCserve Central Host-Based VM Backup).
Wiederherstellen mit einer Hyper-V-Virtual Standby-VM
(Sie können Daten nur wiederherstellen, wenn die virtuelle Konvertierung mit CA ARCserve Central Virtual Standby ausgeführt wurde)
Wiederherstellen mit einer VMware-Virtual Standby-VM
(Sie können Daten nur wiederherstellen, wenn die virtuelle Konvertierung mit CA ARCserve Central Virtual Standby ausgeführt wurde)
Hilfsprogramme
Zurück
Weiter
Abbrechen

5. Klicken Sie auf "Weiter".

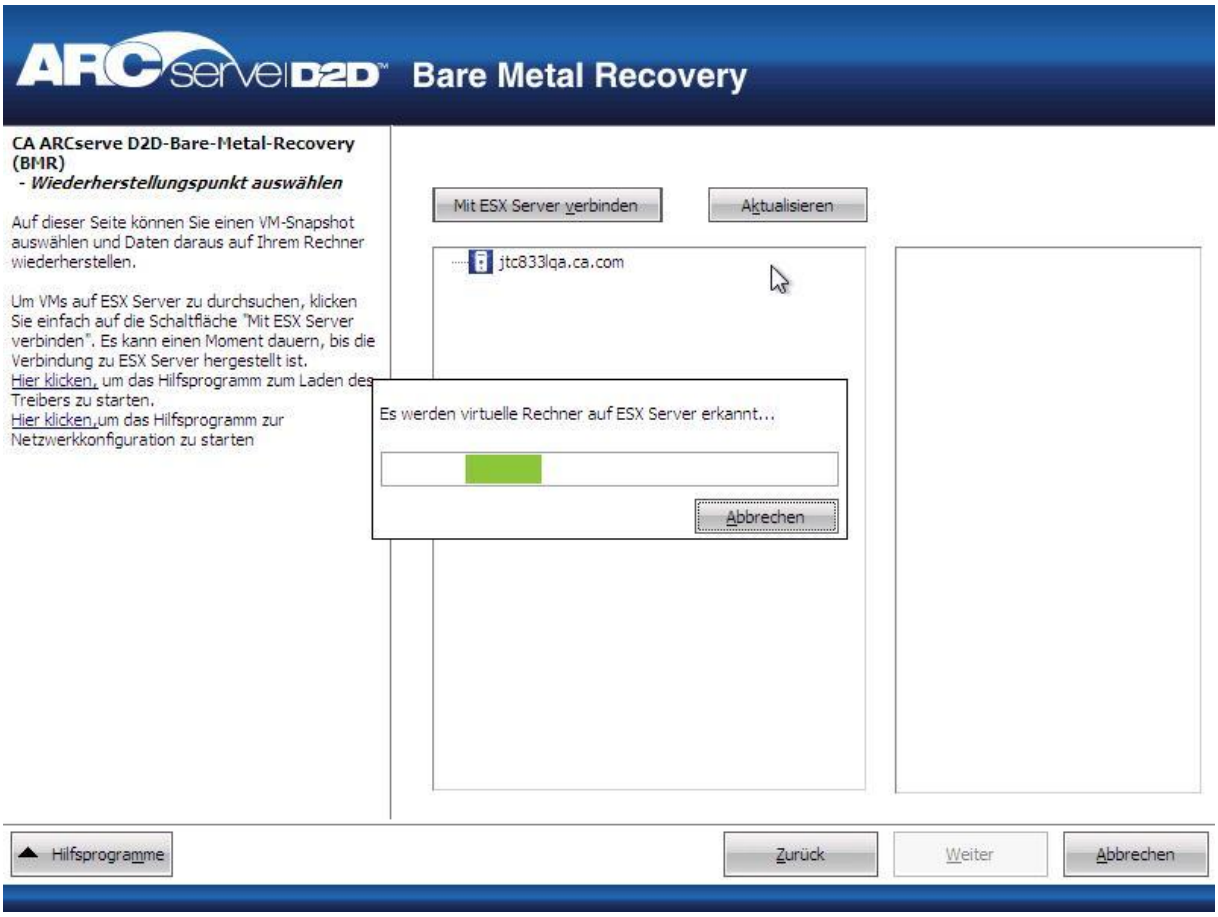
   Das Fenster "Wiederherstellungspunkt auswählen" wird mit dem Dialogfeld "ESX/VC-Anmeldeinformationen" angezeigt.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungspunkt auswählen
Auf dieser Seite können Sie einen VM-Snapshot auswählen und Daten daraus auf Ihrem Rechner wiederherstellen.
Um VMs auf ESX Server zu durchsuchen, klicke Sie einfach auf die Schaltfläche "Mit ESX Serve verbinden". Es kann einen Moment dauern, bis Verbindung zu ESX Server hergestellt ist.
Hier klicken, um das Hilfsprogramm zum Laden Treibers zu starten.
Hier klicken, um das Hilfsprogramm zur Netzwerkkonfiguration zu starten
Mit ESX Server verbinden
Aktualisieren
Geben Sie ESX/vCenter-Anmeldeinformationen ein
ESX Server/vCenter:
Benutzername:
Kennwort:
VI-Port:
443
HTTP
HTTPS
OK
Abbrechen
Hilfsprogramme
Zurück
Weiter
Abbrechen

6. Geben Sie Anmeldeinformationen ein, und klicken Sie auf "OK".

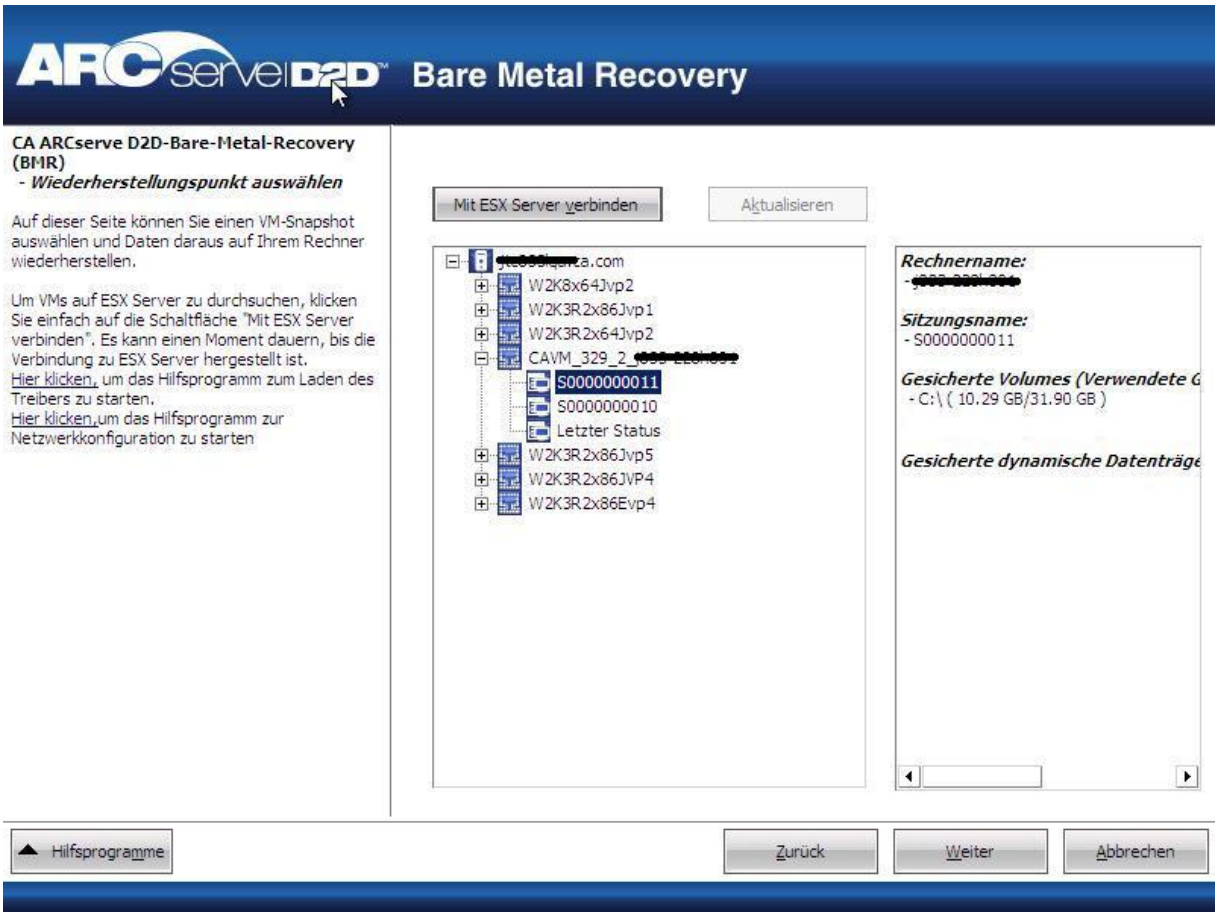
   Das Fenster "Wiederherstellungspunkt auswählen" wird angezeigt.

   CA ARCserve D2D ruft dann alle Wiederherstellungspunkt-Snapshots für den ausgewählten VMware-Server ab und zeigt den VMware-Server im linken Bereich an, mit einer Auflistung aller virtuellen Rechner, die auf dem ausgewählten VMware-Server gehostet werden.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungspunkt auswählen
Auf dieser Seite können Sie einen VM-Snapshot auswählen und Daten daraus auf Ihrem Rechner wiederherstellen.
Um VMs auf ESX Server zu durchsuchen, klicken Sie einfach auf die Schaltfläche "Mit ESX Server verbinden". Es kann einen Moment dauern, bis die Verbindung zu ESX Server hergestellt ist.
Hier klicken, um das Hilfsprogramm zum Laden des Treibers zu starten.
Hier klicken,um das Hilfsprogramm zur Netzwerkkonfiguration zu starten
Mit ESX Server verbinden
Aktualisieren
jtc833lqa.ca.com
Es werden virtuelle Rechner auf ESX Server erkannt...
Abbrechen
Hilfsprogramme
Zurück
Weiter
Abbrechen

7. Wählen Sie den virtuellen Rechner aus, der Wiederherstellungspunkte für Ihr Sicherungs-Image enthält.

   Die Sicherungssitzungen (Wiederherstellungspunkt-Snapshots) für den ausgewählten virtuellen Rechner werden angezeigt.



8. Wählen Sie die Sicherungssitzung des virtuellen Rechners (Wiederherstellungspunkt-Snapshots), die Sie wiederherstellen möchten.

   Die entsprechenden Details für den ausgewählten Wiederherstellungspunkt-Snapshot (Name des virtuellen Rechners, Name der Sicherungssitzung, gesicherte Volumes, gesicherte dynamische Datenträger) werden im rechten Bereich angezeigt.

   Sie können einen der aufgelisteten Wiederherstellungspunkte auswählen und haben dazu noch die Möglichkeit, den Wiederherstellungspunkt "Aktueller Status" oder "Letzter Status" auszuwählen.

   - Wenn der virtuelle Rechner, von dem Sie eine Wiederherstellung durchführen, aktiviert ist, wird der Wiederherstellungspunkt "Aktueller Status" angezeigt.
   - Wenn der virtuelle Rechner, von dem Sie eine Wiederherstellung durchführen, deaktiviert ist, wird der Wiederherstellungspunkt "Letzter Status" angezeigt.

     Wenn Sie den Wiederherstellungspunkt "Letzter Status" auswählen, wird eine Fehlermeldung angezeigt, um Sie darüber zu informieren, dass der Wiederherstellungspunkt, von dem Sie eine Wiederherstellung durchführen, der Status "Letzter Status" (und nicht "Aktueller Status") ist. Es wird verlangt, dass Sie den virtuellen Rechner starten, bevor Sie mit der Wiederherstellung fortfahren.

9. Überprüfen Sie, ob es sich um den gewünschten Wiederherstellungspunkt handelt, und klicken Sie auf "Weiter".

   Im BMR-Assistenten werden die verfügbaren Wiederherstellungsmodi angezeigt.

ARCserve D2D Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungsmodus auswählen
Welchen Wiederherstellungsmodus möchten Sie verwenden?
Express-Modus
Im Express-Modus wird das System automatisch durch nur minimales Eingreifen des Benutzers und die Verwendung der Standardeinstellungen des Rechners wiederhergestellt.
Erweiterter Modus
Der erweiterte Modus unterstützt Sie beim Anpassen des Wiederherstellungsprozesses. Mit diesem Modus können Sie folgende Aktionen ausführen:
Entscheiden, ob Sie Daten auf Basisvolumes oder dynamischen Volumes wiederherstellen möchten.
Gerätetreiber vor dem Neustart einfügen.
Hinweis: Wenn Sie auf 'Weiter' klicken, erstellt der BMR-Assistent neue Partitionen auf dem Zielrechner, die mit den Partitionen auf dem Quellrechner übereinstimmen. Möglicherweise werden Partitionen auf dem Zielrechner gelöscht und neue erstellt.
Hilfsprogramme
Zurück
Weiter
Abbrechen

10. Auswählen des Wiederherstellungsmodus

    Es stehen die Optionen "Erweiterter Modus" und "Express-Modus" zur Verfügung.

    - Wenn Sie den Wiederherstellungsprozess personalisieren möchten, wählen Sie "Erweiterter Modus".
    - Wenn Sie in den Wiederherstellungsprozess minimal eingreifen möchten, wählen Sie "Express-Modus".

    Standard: Express-Modus.

    Hinweis: Der restliche Vorgang gilt nur im erweiterten Modus, und der Vorgang enthält Informationen, die Sie durch die Bare-Metal-Recovery führen.

11. Klicken Sie auf "Weiter".

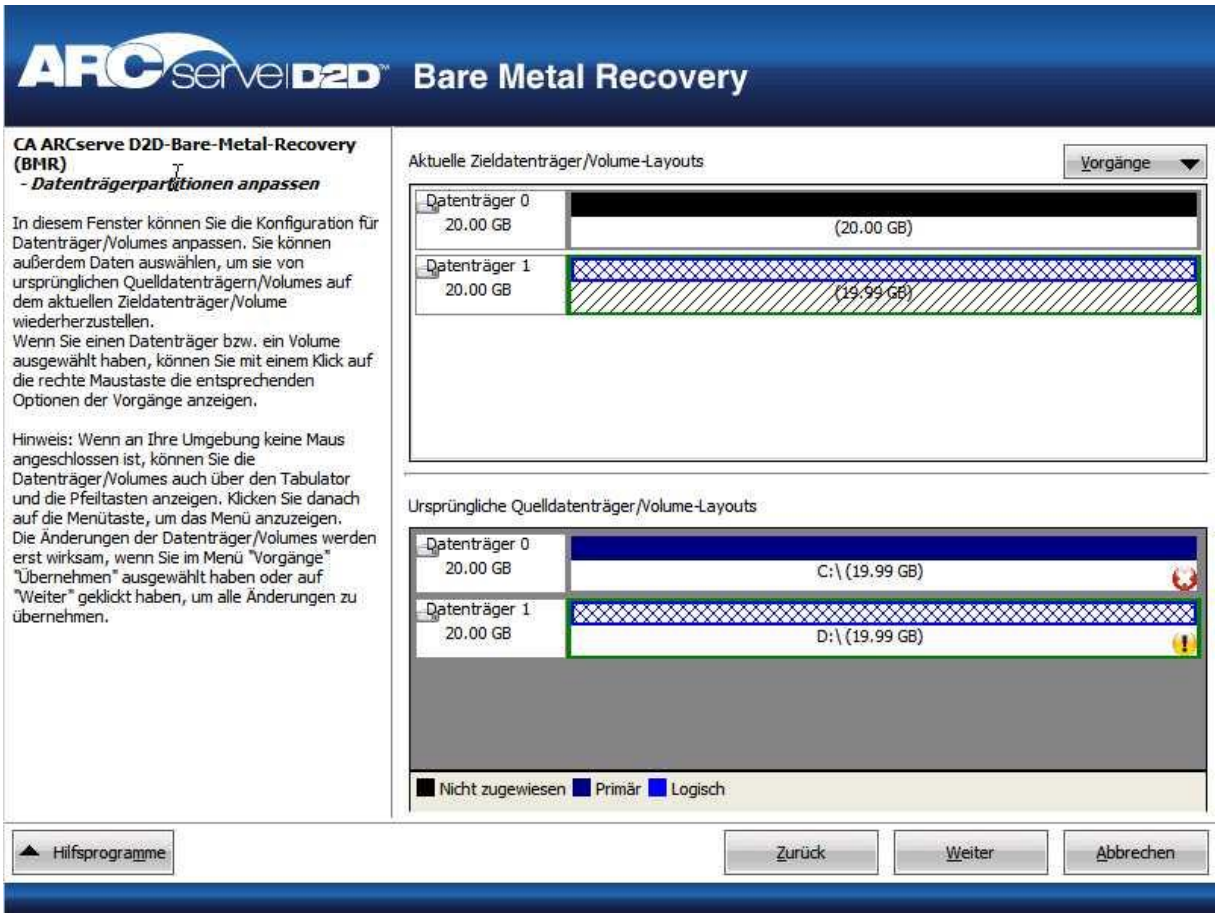
    Das BMR-Hilfsprogramm beginnt mit der Suche nach den wiederherzustellenden Rechnern und zeigt die entsprechenden Informationen zu Datenträgerpartitionen an.

    Im oberen Fensterbereich wird die Datenträgerkonfiguration des derzeitigen Rechners (Zielrechners) angezeigt. Im unteren Fensterbereich wird die Datenträgerkonfiguration angezeigt, die Sie am ursprünglichen Rechner (Quellrechner) eingestellt hatten.

Wichtig! Ein rotes X-Symbol, das für ein Quellvolume im unteren Bereich angezeigt wird, gibt an, dass dieses Volume Systeminformationen enthält und dem Zieldatenträger nicht zugewiesen (zugeordnet) wurde. Diese Systeminformationen müssen dem Zieldatenträger zugewiesen werden und während der Bare-Metal-Recovery wiederhergestellt werden. Anderenfalls schlägt der Neustart fehl.

Hinweis: Wenn Sie eine BMR ausführen und das Systemvolume auf einem Datenträger wiederherstellen, der nicht als Startdatenträger konfiguriert ist, kann der Rechner nicht gestartet werden, nachdem BMR abgeschlossen wurde. Stellen Sie sicher, dass Sie das Systemvolume auf einem ordnungsgemäß konfigurierten Startdatenträger wiederherstellen.

Hinweis: Bei einer Wiederherstellung auf einem anderen Datenträger oder Volume muss die Kapazität des neuen Datenträgers gleich oder größer als die des ursprünglichen Datenträgers/Volumes sein. Datenträger-Größenänderung ist außerdem nur bei Basisdatenträgern möglich, nicht bei dynamischen Datenträgern.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Datenträgerpartitionen anpassen
In diesem Fenster können Sie die Konfiguration für Datenträger/Volumes anpassen. Sie können außerdem Daten auswählen, um sie von ursprünglichen Quelldatenträgern/Volumes auf dem aktuellen Zieldatenträger/Volume wiederherzustellen.
Wenn Sie einen Datenträger bzw. ein Volume ausgewählt haben, können Sie mit einem Klick auf die rechte Maustaste die entsprechenden Optionen der Vorgänge anzeigen.
Hinweis: Wenn an Ihre Umgebung keine Maus angeschlossen ist, können Sie die Datenträger/Volumes auch über den Tabulator und die Pfeiltasten anzeigen. Klicken Sie danach auf die Menütaste, um das Menü anzuzeigen. Die Änderungen der Datenträger/Volumes werden erst wirksam, wenn Sie im Menü "Vorgänge" "Übernehmen" ausgewählt haben oder auf "Weiter" geklickt haben, um alle Änderungen zu übernehmen.
Aktuelle Zieldatenträger/Volume-Layouts
Vorgänge
Datenträger 0
20.00 GB
(20.00 GB)
Datenträger 1
20.00 GB
(19.99 GB)
Ursprüngliche Quelldatenträger/Volume-Layouts
Datenträger 0
20.00 GB
C:\ (19.99 GB)
Datenträger 1
20.00 GB
D:\ (19.99 GB)
Nicht zugewiesen
Primär
Logisch
Hilfsprogramme
Zurück
Weiter
Abbrechen

12. Wenn Ihnen die angezeigten aktuellen Datenträgerinformationen nicht richtig erscheinen, können Sie auf das Menü "Hilfsprogramm" zugreifen und nach eventuell fehlenden Treibern suchen.

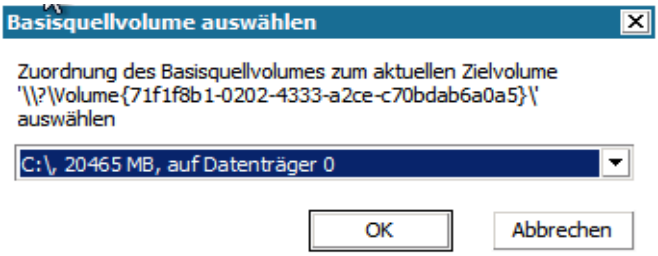
13. Wenn nötig, können Sie im Fensterbereich des Zielvolumes auf das Drop-down-Menü "Vorgänge" klicken, um die verfügbaren Optionen anzuzeigen.

    Von diesem Menü aus können Sie bestehende Partitionen zurücksetzen bzw. neue Partitionen erstellen, um den Datenträgerpartitionen auf dem Quellvolume zu entsprechen. (Zurücksetzen bedeutet, die Informationen zu Quell- und Zieldatenträgerlayout neu aus der Konfigurationsdatei und dem derzeitigen BS zu laden und alle vom Benutzer geänderten Informationen zum Datenträgerlayout zu verwerfen).

    Hinweis: Wenn Sie eine Zuordnung zu einem anderen Datenträger durchführen, muss die Kapazität jedes zugeordneten Zielvolume gleich oder größer als die des entsprechenden Quellvolumes sein.

14. Klicken Sie auf das entsprechende Zielvolume und wählen Sie im Popup-Menü die Option "Volume zuordnen von", um diesem Zielvolume ein Quellvolume zuzuordnen.

    Das Dialogfeld "Basisquellvolume auswählen" wird geöffnet.

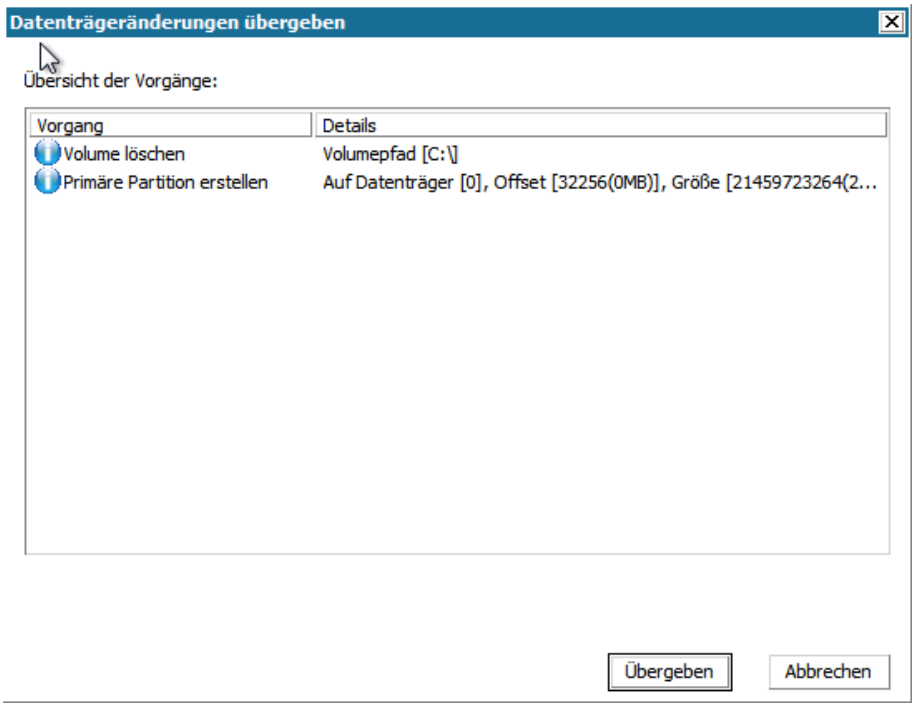


15. Klicken Sie im Dialogfeld "Basisquellvolume auswählen" auf das Drop-down-Menü, und wählen Sie das verfügbare Quellvolume, um es dem ausgewählten Zielvolume zuzuordnen. Klicken Sie auf "OK".

    - Im Zielvolume zeigt ein grünes hakenförmiges Symbol an, dass eine Zuordnung zu diesem Zielvolume durchgeführt wurde.
    - Im Quellvolume zeigt ein rotes x-förmiges Symbol an, dass dieses Quellvolume einem Zielvolume zugeordnet wurde.

16. Wenn Sie sicher sind, dass alle Volumes, die Sie wiederherstellen möchten, und alle Volumes, die Systeminformationen enthalten, einem Zielvolume zugeordnet sind, klicken Sie auf "Weiter".

    Im Bildschirm "Änderungen des Datenträgers übergeben" wird eine Übersicht über die ausgewählten Vorgänge angezeigt. Für jedes neu erstellte Volume werden die entsprechenden Informationen angezeigt.



17. Überprüfen Sie die Übersichtsinformationen, und klicken Sie auf "Übergeben". (Wenn die Informationen nicht richtig sind, klicken Sie auf "Abbrechen").

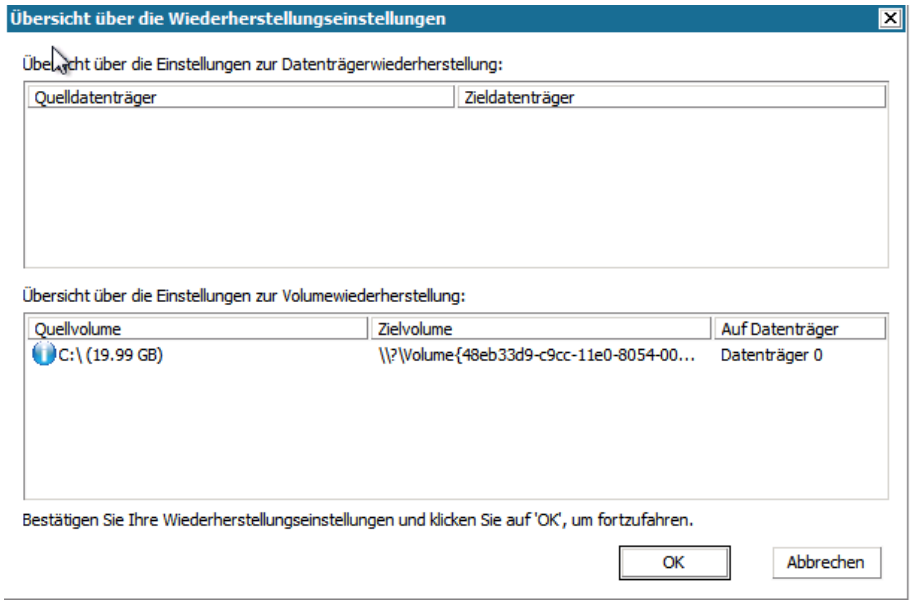
    Hinweis: Sämtliche Vorgänge, die die Festplatte betreffen, werden erst wirksam, wenn Sie sie übergeben haben.

    Auf dem Zielrechner werden die neuen Volumes erstellt und dem entsprechenden Quellrechner zugeordnet.

18. Wenn alle Änderungen abgeschlossen sind, klicken Sie auf "OK".

    Im Bildschirm "Übersicht über die Wiederherstellungseinstellungen" wird eine Übersicht der wiederherzustellenden Volumen angezeigt.

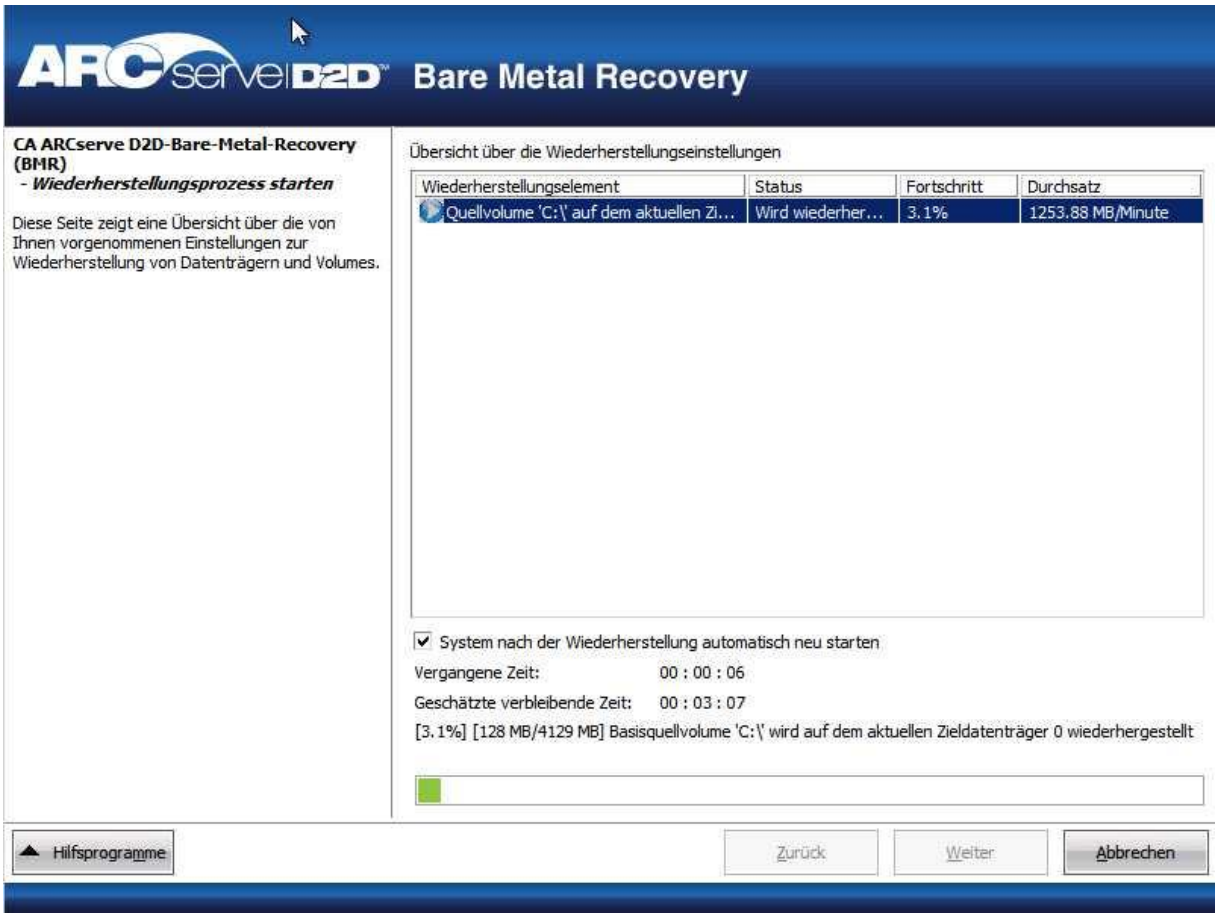
    Hinweis: Die Laufwerkbuchstaben, die unten in der Spalte "Zielvolume" aufgelistet werden, werden von Windows Preinstallation Environment (WinPE) automatisch erstellt. Sie können von den Laufwerkbuchstaben der Spalte "Quellvolume" abweichen. Auch wenn die Laufwerkbuchstaben nicht miteinander übereinstimmen werden die Daten im richtigen Volume ordnungsgemäß wiederhergestellt.



19. Nachdem Sie die Übersichtsinformationen überprüft haben, klicken Sie auf "OK".

    Der Wiederherstellungsprozess beginnt. Im BMR-Assistenten wird der Wiederherstellungsstatus jedes Volumes angezeigt.

    - Dieser Vorgang kann, abhängig von der Größe des Volumes, das wiederhergestellt wird, eine Weile dauern.
    - Sie stellen durch diesen Prozess sämtliche Informationen, die Sie für diesen Wiederherstellungspunkt gespeichert hatten, Block für Block wieder her und erstellen auf dem Zielrechner eine Kopie des Quellrechners.
    - Standardmäßig ist die Option, die nach der Wiederherstellung einen automatischen Systemneustart festlegt, aktiviert. Wenn nötig, können Sie diese Option löschen und den Neustart zu einem späteren Zeitpunkt manuell durchführen.
    - Sie können den Vorgang auch jederzeit abbrechen.


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungsprozess starten
Diese Seite zeigt eine Übersicht über die von Ihnen vorgenommenen Einstellungen zur Wiederherstellung von Datenträgern und Volumes.
Übersicht über die Wiederherstellungseinstellungen
Wiederherstellungselement
Status
Fortschritt
Durchsatz
Quellvolume 'C:\' auf dem aktuellen Zi...
Wird wiederher...
3.1%
1253.88 MB/Minute
System nach der Wiederherstellung automatisch neu starten
Vergangene Zeit: 00 : 00 : 06
Geschätzte verbleibende Zeit: 00 : 03 : 07
[3.1%] [128 MB/4129 MB] Basisquellvolume 'C:\' wird auf dem aktuellen Zieldatenträger 0 wiederhergestellt
Hilfsprogramme
Zurück
Weiter
Abbrechen

20. Über das Hilfsprogramm-Menü können Sie auf das BMR-Aktivitätsprotokoll zugreifen und es mit der Option "Speichern" speichern.

    Der standardmäßige Speicherplatz für das Aktivitätsprotokoll ist folgender:

    X:\windows\system32\dr\log.

    Hinweis: Wenn Sie die Option "Speichern unter" des Fensters "BMR-Aktivitätsprotokoll" verwenden, sollten Sie, um Windows-bedingten Fehlern vorzubeugen, das Aktivitätsprotokoll nicht auf dem Desktop speichern oder einen Ordner auf dem Desktop dafür erstellen.

21. Wenn Sie die Wiederherstellung auf einer abweichenden Hardware durchführen (z. B. wenn der SCSI-/FC-Adapter, der zur Verbindung mit den Festplatten verwendet wurde, geändert wurde), und im ursprünglichen System kein kompatibler Treiber gefunden wird, wird die Seite "Treibereinfügung" angezeigt, über die Sie sich mit den benötigten Treibern versorgen können.

    Sie können das System durchsuchen und einzufügende Treiber auswählen, sodass sogar ein Rechner mit anderer Hardware nach einer Bare-Metal-Recovery wiederhergestellt werden kann.

22. Nach Abschluss der Bare-Metal-Recovery wird eine Bestätigungsmeldung angezeigt.

Hinweise: Nach Abschluss der BMR:

- Die erste Sicherung, die ausgeführt wird, ist eine Überprüfungssicherung.
- Wenn die Bare-Metal-Recovery abgeschlossen ist, sollten Sie überprüfen, ob das BIOS so konfiguriert ist, dass der Start vom Datenträger, auf dem das Boot-Volume wiederhergestellt wurde, durchgeführt wird.
- Wenn Sie auf abweichender Hardware wiederhergestellt haben, müssen Sie die Netzwerkadapter nach dem Neustart des Rechners möglicherweise manuell konfigurieren.
- Bei dynamischen Datenträgern können Sie den Offline-Status des Datenträgers über die Datenträgerverwaltung manuell in online umändern (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).
- Sie können dynamische Volumes auf dynamischen Datenträgern, die aufgrund von Redundanz fehlgeschlagen sind, über die Datenträgerverwaltung manuell neu synchronisieren (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).

Wiederherstellen von Microsoft Exchange-E-Mail-Nachrichten

Virtual Standby ermöglicht es Ihnen, Microsoft Exchange-Daten aus CA ARCserve D2D-Wiederherstellungspunkten wiederherzustellen. Von den Wiederherstellungspunkten können Sie Postfächer, Postfachordner und individuelle E-Mail-Nachrichten wiederherstellen.

Hinweis: Um spezifische Wiederherstellungen von Exchange-Serverdaten auszuführen, muss Ihr Konto über die erforderlichen Zugriffsberechtigungen verfügen. Weitere Informationen finden Sie im *CA ARCserve D2D-Benutzerhandbuch*.

So stellen Sie Microsoft Exchange-E-Mail-Nachrichten wieder her

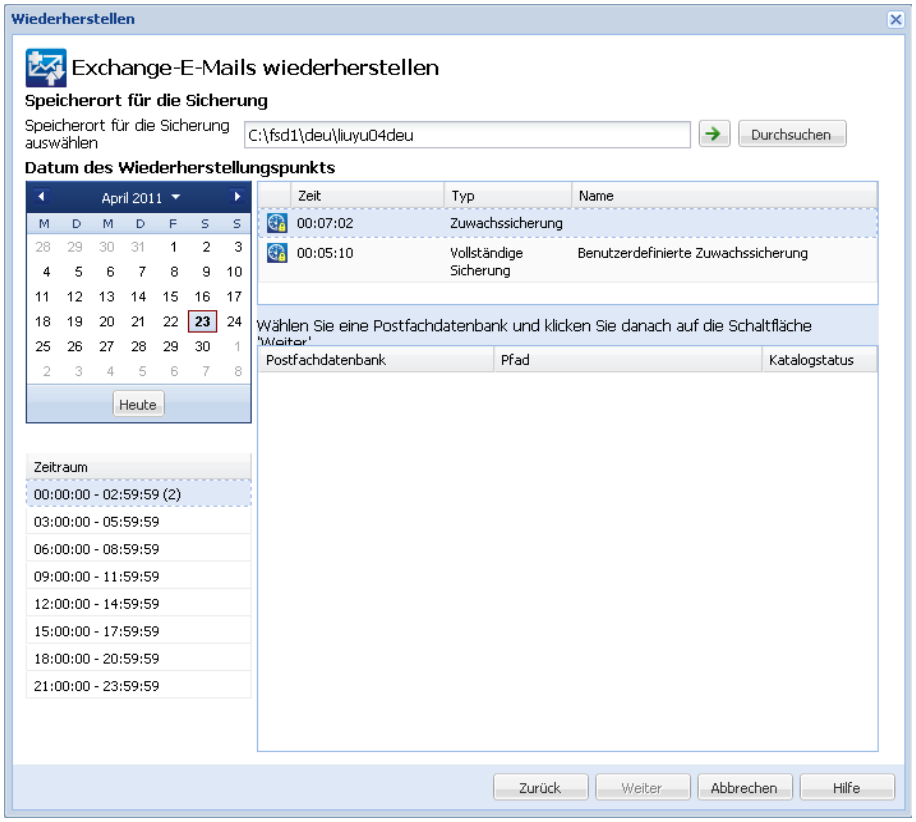
1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".

2. Klicken Sie vom Dialogfeld "Wiederherstellen" auf "Exchange-E-Mails wiederherstellen".

   Das Dialogfeld "Exchange-E-Mails wiederherstellen" wird geöffnet.



3. Geben Sie den Speicherort für die Sicherung an. Sie können den Speicherort der Sicherungs-Images angeben oder das System danach durchsuchen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten. Klicken Sie auf das grüne Pfeilsymbol, um zu überprüfen, ob ein ordnungsgemäßer Zugriff auf den Speicherort der Sicherungsquelle besteht.

   Im Kalender sind alle Daten für die angezeigte Zeitspanne, die Wiederherstellungspunkte für diese Sicherungsquelle enthalten, grün hervorgehoben.

4. Geben Sie das Datum für das Sicherungs-Image an, das Sie wiederherstellen möchten.

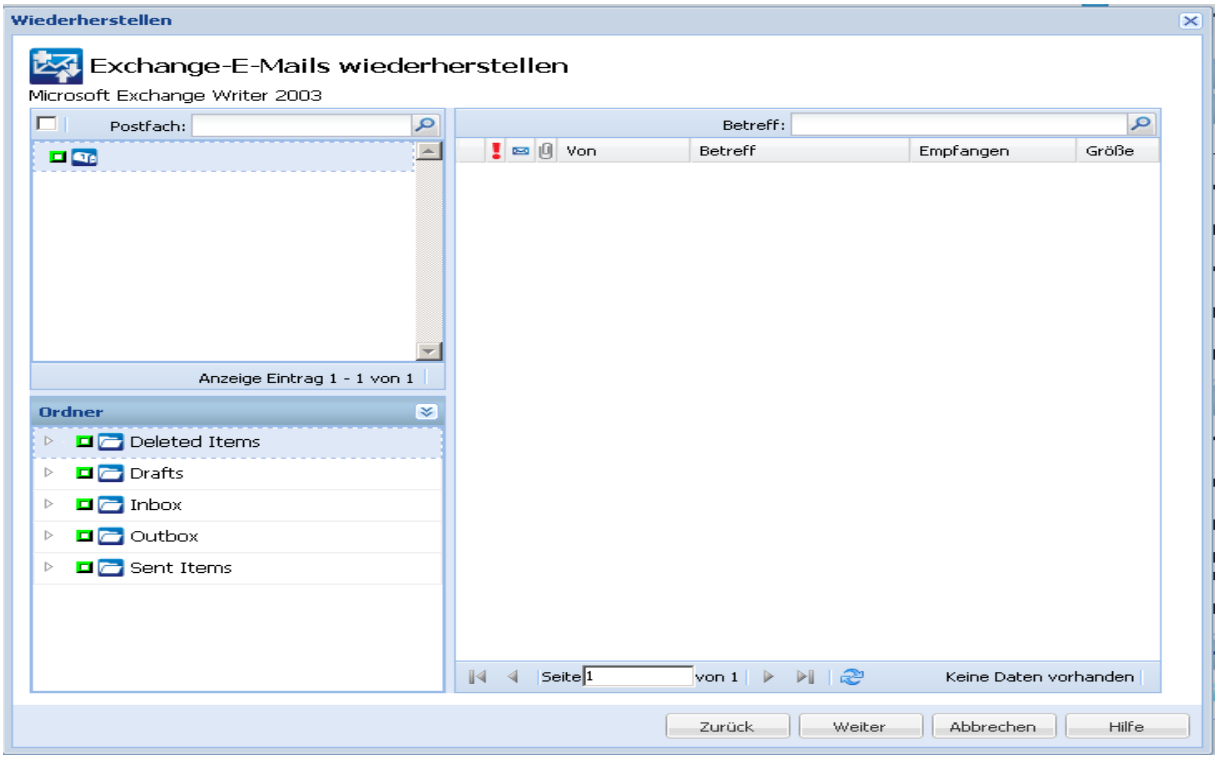
   Es werden die entsprechenden Exchange-Postfachdatenbanken einschließlich Uhrzeit, Sicherungstyp und Name der Sicherung angezeigt.

5. Wählen Sie eine Exchange-Postfachdatenbank, die Sie wiederherstellen möchten, und klicken Sie auf "Weiter".

   Hinweis: Wenn Sie während der Sicherung (kein generierter Katalog) die Option "Spezifische Wiederherstellung von Exchange-Objekten" aktiviert haben, wird eine Benachrichtigung angezeigt, in der Sie angeben müssen, ob Sie derzeitig einen Katalog für die spezifische Wiederherstellung von Exchange-Objekten generieren möchten. Wenn Sie bei der Generierung des Katalogs "Nein" auswählen, werden Sie keine detaillierten Wiederherstellungspunkte durchsuchen oder auswählen können. Dadurch können Sie eine vollständige Datenbankwiederherstellung nur über das Dialogfeld "Wiederherstellungspunkte durchsuchen" durchführen.

   Das Dialogfeld "Exchange-E-Mails wiederherstellen" ist aktualisiert, um eine Auflistung des Postfachinhalts für die ausgewählte Datenbank anzuzeigen.

   Hinweis: Spezifische Wiederherstellung von Exchange unterstützt lediglich E-Mail-Wiederherstellungen. Wiederherstellungen von Kalendern, Kontakten, Notizen und Tasks werden nicht unterstützt.



6. Wählen Sie die Ebene der wiederherzustellenden Exchange-Objekte aus (Postfach, Ordner oder individuelle Mail).

   Sie können den gesamten Inhalt oder Teile des Inhalts des wiederherzustellenden Exchange-Objekts auswählen. Sie können mehrere wiederherzustellende Exchange-Objekte auswählen.

   Hinweis: CA ARCserve D2D unterstützt die spezifische Wiederherstellung von öffentlichen Exchange-Ordnerobjekten nicht. Sie müssen die Wiederherstellung auf Anwendungsebene verwenden, um die ganze Datenbank der öffentlichen Ordner wiederherzustellen und dann das spezifische Exchange-Objekt extrahieren, das Sie benötigen.

   Hinweis: Wenn CA ARCserve D2D verwendet wird, um individuelle Postfach-/Mail-Objekte von der Exchange-Postfachdatenbank wiederherzustellen, muss das Betriebssystem, das für die Wiederherstellung verwendet wurde, mit dem Betriebssystem, das für die Sicherung verwendet wurde, übereinstimmen (einschließlich derselben Windows-Versionsnummer und Service Pack-Ebene sowie der entsprechend zur Unterstützung erforderlichen Version des Visual C++ Redistributable Package).

   Hinweis: Während Sie E-Mails in der CA ARCserve D2D-Benutzeroberfläche durchsuchen und wiederherstellen, wird möglicherweise die Feldeigenschaft "Von" in der Benutzeroberfläche für Postfächer, die noch nicht beim Exchange Server angemeldet wurden, nicht angezeigt. In diesem Fall werden die E-Mails dennoch ordnungsgemäß wiederhergestellt.

   a. Sie können eine Postfachdatenbank auswählen.

      Wenn Sie eine Postfachdatenbank auswählen, werden alle Postfächer in dieser Datenbank wiederhergestellt.

   b. Sie können das wiederherzustellende Postfach (oder Postfächer) auswählen.

      Wenn Sie eine Postfachebene auswählen, wird der gesamte entsprechende Inhalt (Ordner und individuelle Mail) innerhalb des Postfachs wiederhergestellt.

   c. Sie können einen oder mehrere Ordner innerhalb eines ausgewählten wiederherzustellenden Postfachs wählen.

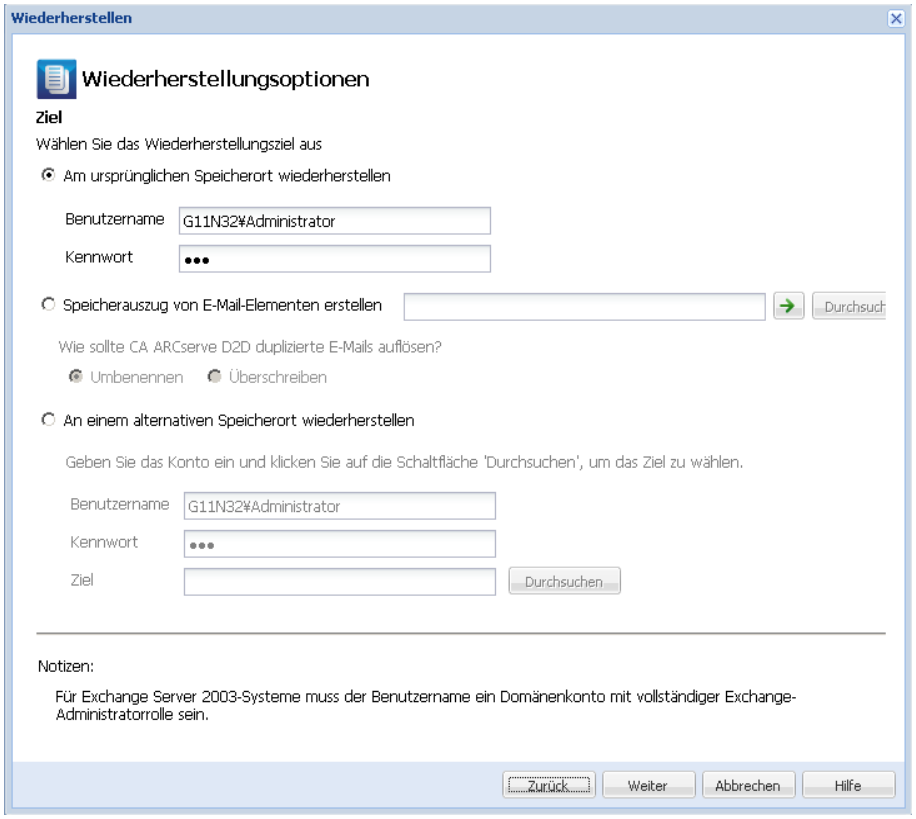
      Wenn Sie die Postfachordnerebene auswählen, wird der gesamte entsprechende Mail-Inhalt innerhalb des Ordners wiederhergestellt.

   d. Sie können die individuell wiederherzustellenden Mails auswählen.

      Wenn Sie die individuelle Mail-Ebene auswählen, werden nur die ausgewählten Mail-Objekte wiederhergestellt.

      Hinweis: Für Exchange 2003 gilt, wenn die wiederherzustellende Mail über einen anderen E-Mail-Client als Outlook gesendet wurde und die Mail bei der Sicherung über einen Kennzeichnungsstatus verfügt hat, wird die Mail selbst zwar wiederhergestellt, aber die angehangene Markierung wird nicht mit eingeschlossen.

7. Wenn die wiederherzustellenden Exchange-Objekte angegeben sind, klicken Sie auf "Weiter".



8. Wählen Sie das Ziel für die Wiederherstellung aus.

   Die verfügbaren Optionen können am ursprünglichen Speicherort der Sicherung, oder an einem anderen Speicherort wiederhergestellt werden.

   Hinweis: Für Exchange 2010 können archivierte Postfachelemente nicht am ursprünglichen Speicherort wiederhergestellt werden. Archivierte Postfachelemente können nur an einem alternativen Speicherort oder auf einem lokalen Datenträger wiederhergestellt werden. Außerdem können normale Postfachelemente nicht wiederhergestellt werden, um Postfächer zu archivieren.

Am ursprünglichen Speicherort wiederherstellen

Stellt die E-Mails am selben Speicherort wieder her, an dem das Sicherungs-Image erstellt wurde. Mails behalten die gleiche Hierarchie bei und werden am ursprünglichen Postfach und im ursprünglichen Ordner wiederhergestellt.

- Wenn der derzeitige Rechner nicht der aktive Exchange-Server ist, wird CA ARCserve D2D den Speicherort des aktiven Servers erkennen und die Mails auf dem aktiven Server wiederherstellen.
- Wenn das Postfach innerhalb derselben Organisation auf einem anderen Exchange-Server verschoben wurde, erkennt CA ARCserve D2D den neuen Exchange Server, auf dem sich das ursprüngliche Postfach befindet und führt die Wiederherstellung auf dem neuen Server durch.
- Wenn der Anzeigename des Postfachs geändert wurde, kann das Postfach (von einer früheren Sicherungssitzung) nicht am ursprünglichen Speicherort wiederhergestellt werden, da CA ARCserve D2D den geänderten Namen nicht finden kann. Um dieses Problem zu lösen, können Sie angeben, dass dieses Postfach an einem alternativen Speicherort wiederhergestellt werden soll.

Hinweis: Beim Wiederherstellen eines Postfachs oder einer E-Mail am ursprünglichen Speicherort sollten Sie sich vergewissern, dass das Zielpostfach verfügbar ist. Anderenfalls schlägt die Wiederherstellung fehl.
CA ARCserve D2D validiert das Ziel nur dann, wenn der Wiederherstellungsjob übergeben wird.

Nur Speicherauszugsdatei

Stellt die E-Mails auf einem Datenträger wieder her. Dieser Speicherort kann ein lokaler Rechner oder ein Remote-Rechner sein. Die wiederhergestellten E-Mails behalten dieselbe Hierarchie, die sie im entsprechenden Exchange-Postfach hatten. Der Dateiname wird der Betreff der E-Mail sein.

Hinweis: Wenn der E-Mail-Betreff, der Ordnername oder der Postfachname einen der folgenden Zeichen enthält, wird das Zeichen durch einen Bindestrich (-) im Dateinamen ersetzt: \ / : * ? " < > |

Für diese Option müssen Sie ebenfalls angeben, was CA ARCserve D2D vornehmen soll, um eine Konfliktsituation zu lösen. In Exchange können Sie mehrere Mail-Objekte mit demselben Namen unter dem gleichen Ordner haben. Allerdings können in einem Dateisystem zwei Dateien mit demselben Namen nicht unter dem gleichen Ordner vorhanden sein.

Es gibt zwei Optionen, um diese Konfliktsituation zu lösen:

- **Umbenennen**: Falls auf dem Datenträger eine Datei vorhanden ist, deren Name mit dem E-Mail-Betreff übereinstimmt, benennt CA ARCserve D2D den E-Mail-Betreff und hängt am Ende des Betreffs eine Zahl an.
- **Überschreiben**: Falls auf dem Datenträger eine Datei vorhanden ist, deren Name mit dem E-Mail-Betreff übereinstimmt, überschreibt CA ARCserve D2D diese Datei.

Hinweis: Wenn Sie individuelle Mailobjekte auswählen, um sie auf der Festplatte wiederherzustellen (Dump), ist das Format des wiederhergestellten Mailobjekts standardmäßig eine Outlook-Nachricht-Datei (.MSG) und nicht eine Datei im Format "Personal Storage Table" (.PST).

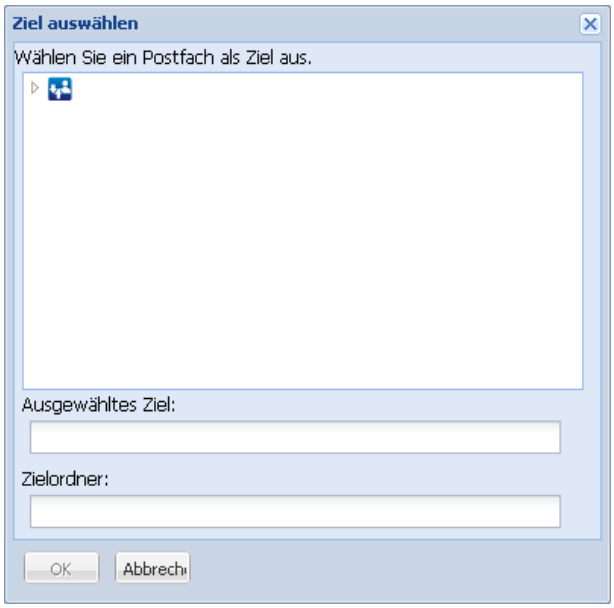
An einem alternativen Speicherort wiederherstellen:

Stellt die Mails an einem angegebenen Speicherort wieder her oder ermöglicht es Ihnen, den Speicherort zu durchsuchen, an dem Ihre Sicherungs-Images wiederhergestellt werden. Das Ziel muss ein Postfach in der gleichen Exchange-Organisation sein und ein neuer Ordnername ist erforderlich. (Wenn Sie versuchen, Mails an einem alternativen Speicherort wiederherzustellen, kann das Ziel kein öffentlicher Ordner sein)

Hinweis: Wenn Sie Mails an einem alternativen Speicherort wiederherstellen, wird die Wiederherstellung fortgesetzt, falls der angegebene Zielordner bereits vorhanden ist. Wenn der angegebene Ordner nicht vorhanden ist, erstellt CA ARCserve D2D den Ordner zuerst und fährt dann mit der Wiederherstellung fort.

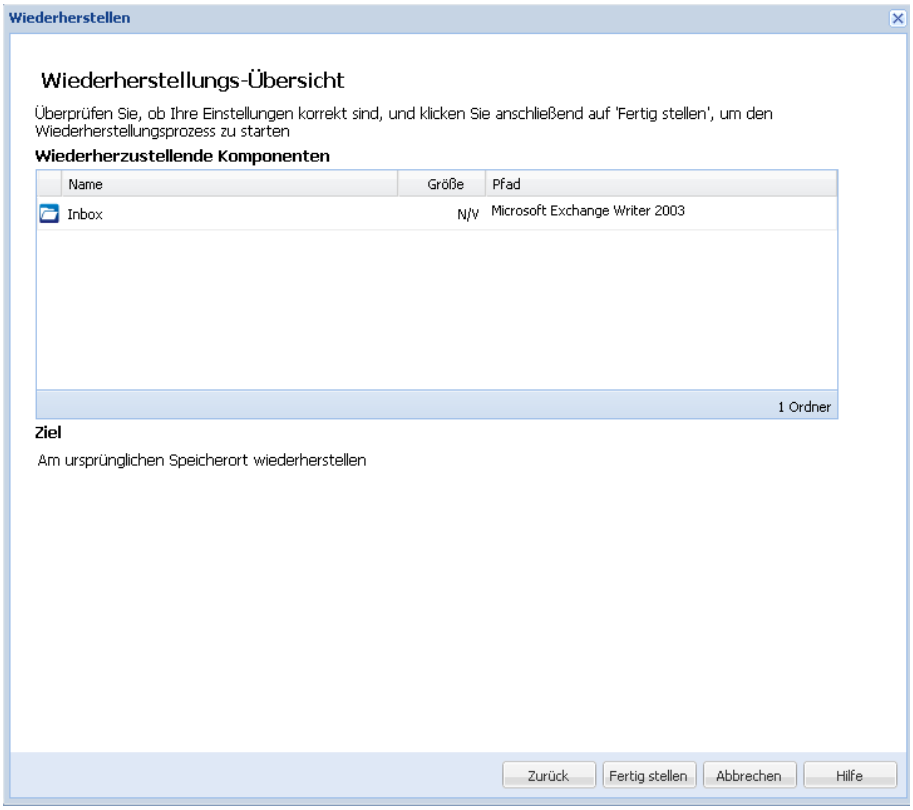
Nachdem Sie den Benutzernamen und das Kennwort eingegeben haben, können Sie auf die Schaltfläche "Durchsuchen" klicken, um durch eine Liste aller Exchange-Server, Speichergruppen, Exchange-Datenbanken und Postfächern in der aktuellen Organisation zu navigieren.

Wählen Sie ein beliebiges Postfach als Ziel aus.



9. Wenn Sie Ihre Wiederherstellungsoptionen ausgewählt haben, klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungs-Übersicht" wird angezeigt.



10. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.

    - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
    - Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

    Hinweis: Wenn der Katalog- und Wiederherstellungsjob für die spezifische Wiederherstellung von Exchange-Objekten in Bearbeitung ist, wird sich die Sicherungssitzung im geladenen Status befinden. Führen Sie auf diesem geladenen Volume keine Vorgänge aus (Formatieren, Laufwerksbuchstaben ändern, Partitionen löschen usw.).

Ändern des Server-Kommunikationsprotokolls

CA ARCserve Central Applications verwendet standardmäßig Hypertext Transfer Protocol (HTTP) zur Kommunikation zwischen seinen Komponenten. Wenn Ihnen eine sichere Übertragung von Kennwörtern zwischen den Komponenten wichtig ist, wählen Sie das Protokoll Hypertext Transfer Protocol Secure (HTTPS). Wenn Sie dagegen diese zusätzliche Sicherheitsstufe nicht benötigen, können Sie das Protokoll ganz einfach wieder auf HTTP zurücksetzen.

Gehen Sie wie folgt vor:

1. Melden Sie sich über ein Administratorkonto oder ein Konto mit Administratorrechten bei dem Computer an, auf dem die Anwendung installiert ist.

   Hinweis: Wenn Sie sich nicht über ein Administratorkonto oder ein Konto mit Administratorrechten anmelden, konfigurieren Sie die Befehlszeile so, dass sie mit dem Recht "Als Administrator ausführen" ausgeführt wird.

2. Öffnen Sie die Windows-Befehlszeile.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - **So ändern Sie das Protokoll von HTTP auf HTTPS:**

     Starten Sie das Hilfsprogramm-Tool "changeToHttps.bat" von folgendem Standardspeicherort (der Speicherort des Ordners 'BIN' kann variieren, je nach dem, wo Sie die Anwendung installiert haben):

     ```
     C:\Programme\CA\ARCserve Central Applications\BIN
     ```

     Wenn das Protokoll erfolgreich geändert wurde, wird die folgende Meldung angezeigt:

     ```
     Das Kommunikationsprotokoll wurde auf HTTPS geändert.
     ```

   - **So ändern Sie das Protokoll von HTTPS auf HTTP:**

     Starten Sie das Hilfsprogramm-Tool "changeToHttp.bat" von folgendem Standardspeicherort (der Speicherort des Ordners 'BIN' kann variieren, je nach dem, wo Sie die Anwendung installiert haben):

     ```
     C:\Programme\CA\ARCserve Central Applications\BIN
     ```

     Wenn das Protokoll erfolgreich geändert wurde, wird die folgende Meldung angezeigt:

     ```
     Das Kommunikationsprotokoll wurde auf HTTP geändert.
     ```

4. Starten Sie den Browser neu und stellen Sie die Verbindung zu CA ARCserve Central Applications neu her.

   Hinweis: Wenn Sie das Protokoll auf HTTPS ändern, wird im Webbrowser eine Warnung angezeigt. Dieses Verhalten tritt wegen eines selbstsignierten Sicherheitszertifikats auf, das Sie auffordert, die Warnung zu ignorieren und fortzufahren, oder dieses Zertifikat zum Browser hinzuzufügen, um dieser Warnung künftig vorzubeugen.

Kapitel 5: Fehlerbehebung in CA ARCserve Central Virtual Standby

Dieser Abschnitt enthält Informationen zur Fehlerbehebung, mit deren Hilfe Sie Probleme erkennen und lösen können, die bei der Verwendung von CA ARCserve Central Virtual Standby möglicherweise auftreten.

Dieses Kapitel enthält folgende Themen:

Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist. (siehe Seite 182)
Leere Webseiten oder JavaScript-Fehler treten auf (siehe Seite 184)
Beheben von Problemen beim Laden von Seiten (siehe Seite 186)
Bei der Anmeldung in CA ARCserve D2D-Knoten und -Überwachungsserver werden Webseiten nicht richtig geladen (siehe Seite 187)
Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift. (siehe Seite 188)
CA ARCserve D2D-Webservice schlägt auf CA ARCserve D2D-Knoten fehl (siehe Seite 189)
Der CA ARCserve D2D-Webservice wird nur langsam ausgeführt. (siehe Seite 192)
CA ARCserve Central Virtual Standby kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen. (siehe Seite 194)
Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt. (siehe Seite 195)
Beim Hinzufügen von Knoten werden ungültige Anmeldeinformationen angezeigt. (siehe Seite 196)
Meldungen zu ungültigen Anmeldeinformationen unter Windows XP (siehe Seite 197)
Fehler wegen verweigerten Zugriffs beim Hinzufügen eines Knotens nach IP/Namen (siehe Seite 198)
Knoten werden nach einer Namensänderung nicht mehr im Bildschirm "Knoten" angezeigt (siehe Seite 200)
Fehler "Operating System Not Found" treten auf (siehe Seite 201)
Virtual Standby-Jobs an Hyper-V-Systeme schlagen fehl (siehe Seite 202)
Virtual Standby-Jobs schlagen aufgrund interner Fehler fehl (siehe Seite 202)
Virtual Standby-Jobs im Hotadd-Transportmodus schlagen fehl (siehe Seite 205)
Virtual Standby-Jobs enden Mit Warnmeldungen zu fehlenden Sitzungen (siehe Seite 207)
Sicherungs- und Wiederherstellungsjobs verwenden den SAN-Transportmodus nicht (siehe Seite 208)
Bei Sicherungen und Wiederherstellungen im Hotadd-Transportmodus werden Datenträger nicht geladen (siehe Seite 210)

Fehlernummern der Fehlerbehebung (siehe Seite 211)
Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet (siehe Seite 212)
Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer 8 und 9 nicht ordnungsgemäß geöffnet (siehe Seite 215)
Bei der Verwendung einer japanischen Tastatur können in Filterfeldern keine Sternchen und Unterstriche als ein Platzhalter verwendet werden (siehe Seite 216)
Virtuelle Rechner nicht automatisch eingeschaltet (siehe Seite 216)

Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist.

Gültig auf Windows-Plattformen.

Symptom:

Wenn Sie versuchen, Knoten über den Bildschirm "Knoten" hinzuzufügen oder zu verbinden, wird folgende Meldung angezeigt:

```
Es kann keine Verbindung zum festgelegten Server hergestellt werden.
```

Lösung:

Wenn diese Meldung angezeigt wird, wenn Sie am Bildschirm "Knoten" Knoten hinzufügen möchten, können die folgenden korrigierenden Maßnahmen bei der Problemlösung helfen:

- Stellen Sie sicher, dass der Windows Server-Dienst auf dem CA ARCserve Central Virtual Standby-Server und auf dem virtuellen Quellrechner (dem Knoten) ausgeführt wird.
- Stellen Sie sicher, dass auf den Datei- und Druckerfreigabedienst von Windows auf dem CA ARCserve Central Virtual Standby-Server und auf dem virtuellen Quellrechner (dem Knoten) eine Windows-Firewallausnahme angewendet ist.
- Stellen Sie sicher, dass auf den Windows-Anmeldedienst nur dann eine Windows-Firewallausnahme angewendet ist, wenn der Knoten kein Mitglied einer Domäne ist. Führen Sie diesen Vorgang sowohl auf dem CA ARCserve Central Virtual Standby-Server als auch auf dem virtuellen Quellrechner (dem Knoten) durch.

- Stellen Sie sicher, dass dem Modul "Freigabe und Sicherheit" des lokalen Kontos der Wert "Klassisch" zugeordnet ist. Gehen Sie wie folgt vor, um den Wert "Klassisch" anzuwenden:

  Hinweis: Führen Sie die folgenden Schritte sowohl auf dem CA ARCserve Central Virtual Standby-Server als auch auf dem virtuellen Quellrechner (dem Knoten) durch.

  1. Melden Sie sich beim CA ARCserve Central Virtual Standby-Server an, und öffnen Sie die Systemsteuerung.
  2. Öffnen Sie in der Systemsteuerung "Verwaltung".
  3. Doppelklicken Sie auf "Lokale Sicherheitsrichtlinie".

     Das Fenster "Lokale Sicherheitsrichtlinie" wird geöffnet.
  4. Erweitern Sie im Fenster "Lokale Sicherheitsrichtlinie" "Sicherheitsoptionen".

     Die Sicherheitsrichtlinien werden angezeigt.
  5. Klicken Sie mit der rechten Maustaste auf "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten", und klicken Sie im Pop-up-Menü auf "Eigenschaften".

     Das Dialogfeld "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten" wird geöffnet.
  6. Klicken Sie auf "Lokale Sicherheitseinstellung".

     Wählen Sie aus der Drop-down-Liste "Klassisch - lokale Benutzer authentifizieren sich als sie selbst" aus.

     Klicken Sie auf "OK".

- Stellen Sie sicher, dass der auf die lokalen Richtlinien für die LAN Manager-Authentifizierungsebene angewendete Wert festgelegt wird, um LM & NTLMv2 zu senden. Verwenden von NTLMv2-Sitzungssicherheit, wenn diese verhandelt wurde. Gehen Sie wie folgt vor, um den Wert anzuwenden:

  1. Melden Sie sich beim CA ARCserve Central Virtual Standby-Server an, und öffnen Sie die Eingabeaufforderung.

     Führen Sie den folgenden Befehl aus:

     ```
     secpol.msc
     ```

     Das Dialogfeld "Lokale Sicherheitseinstellungen" wird geöffnet.
  2. Wählen Sie lokale Einstellungen aus, und klicken Sie auf die Sicherheitsoptionen.

     Suche nach Netzwerksicherheit: LAN Manager-Authentifizierungsebene.

     Doppelklicken Sie auf die Option.

     Das Dialogfeld "Eigenschaften" wird geöffnet.

3. Wählen Sie die entsprechende Option aus, und klicken Sie auf "OK".

   `Senden Sie LM & NTLMv2 - Verwenden Sie NTLMv2-Sitzungssicherheit, wenn diese verhandelt wurde`

4. Führen Sie in der Eingabeaufforderung folgenden Befehl aus:

   `gpupdate`

Der Wert wird angewendet.

Leere Webseiten oder JavaScript-Fehler treten auf

Gültig für Windows Server 2008- und Windows Server 2003-Betriebssysteme.

Symptom:

Wenn Sie CA ARCserve Central Applications-Websites in Internet Explorer öffnen, werden leere Webseiten angezeigt, oder es treten JavaScript-Fehler auf. Das Problem tritt auf, wenn Internet Explorer unter Windows Server 2008- und Windows Server 2003-Betriebssystemen geöffnet wird.

Dieses Problem tritt unter den folgenden Bedingungen auf:

- Sie verwenden Internet Explorer 8 oder Internet Explorer 9, um Ihre Anwendung anzuzeigen, und der Browser erkennt die URL nicht als vertrauenswürdige Seite an.
- Sie verwenden Internet Explorer 9, um Ihre Anwendung anzuzeigen, und verwenden dabei als Übertragungsprotokoll HTTPS.

Lösung:

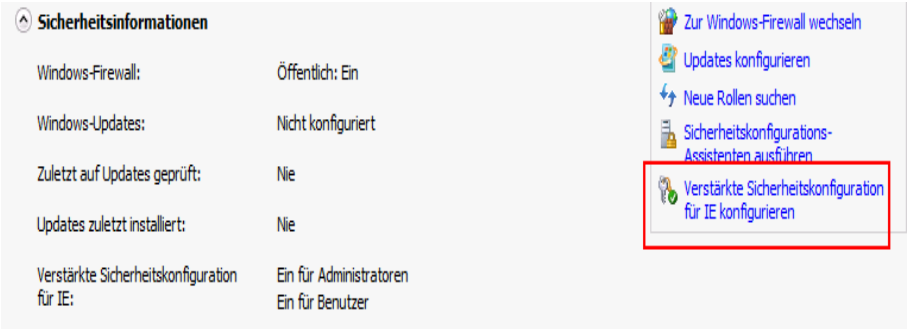
Um dieses Problem zu korrigieren, deaktivieren Sie auf den Computern, die Sie für die Anzeige der Anwendung verwenden möchten, die verstärkte Sicherheitskonfiguration für Internet Explorer.

Um die verstärkte Sicherheitskonfiguration für Internet Explorer unter Windows Server 2008-Systemen zu deaktivieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2008-Computer, den Sie für die Berichtsanzeige verwenden, über das Administratorkonto oder ein Konto mit administrativen Berechtigungen an.
2. Klicken Sie mit der rechten Maustaste auf dem Desktop auf "Computer", und klicken Sie anschließend auf "Verwalten", um das Fenster "Server-Manager " zu öffnen.

3. Klicken Sie im Fenster "Server-Manager " auf "Server-Manager (Servername)".

   Öffnen Sie "Sicherheitsinformationen" im Abschnitt "Serverübersicht", und klicken Sie auf "Verstärkte Sicherheitskonfiguration für IE konfigurieren":



   Das Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" wird geöffnet.

4. Gehen Sie im Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" folgendermaßen vor:

   - Deaktivieren Sie "Administratoren".
   - Deaktivieren Sie "Benutzer".

   Klicken Sie auf "OK".

Das Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" wird geschlossen, und die verstärkte Sicherheit Internet Explorer Sicherheit ist deaktiviert.

Um die verstärkte Sicherheitskonfiguration für Internet Explorer unter Windows Server 2003-Systemen zu deaktivieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2003-Computer, den Sie für die Berichtsanzeige verwenden, über das Administratorkonto oder ein Konto mit administrativen Berechtigungen an.
2. Öffnen Sie die Windows-Systemsteuerung, und öffnen Sie "Software".
3. Klicken Sie im Dialogfeld "Software" auf die Option für Windows-Komponenten "Hinzufügen/Entfernen", um auf den Assistenten für Windows-Komponenten zuzugreifen.

   Entfernen Sie dass das Häkchen neben "Verstärkte Sicherheitskonfiguration für Internet Explorer".

   Klicken Sie auf "Weiter".

   Folgen Sie den Anweisungen auf dem Bildschirm, um die Konfiguration abzuschließen, und klicken Sie auf "Fertig stellen".

Die verstärkte Sicherheit für Internet Explorer wird deaktiviert.

Beheben von Problemen beim Laden von Seiten

Gültig auf Windows-Plattformen.

Symptom:

Die folgenden Fehlermeldungen werden in Browserfenstern angezeigt, wenn Sie sich bei CA ARCserve Central Applications-, CA ARCserve D2D-Knoten und Überwachungsserver anmelden.

Meldung 1:

```
Fehler auf dieser Webseite können zu Fehlern bei der Ausführung führen.
```

Meldung 2:

```
!
```

Lösung:

Webseiten werden aus verschiedenen Gründen nicht richtig geladen. Die folgende Tabelle beschreibt häufige Gründe und die entsprechenden Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Es gibt Probleme mit dem zugrunde liegenden HTML-Quellcode.	Aktualisieren Sie die Webseite und versuchen Sie es erneut.
Ihr Netzwerk blockiert "Active Scripting", ActiveX oder Java-Programme.	Lassen Sie zu, dass Ihr Browser "Aktive Scripting", ActiveX oder Java-Programme verwendet.
Ihre Antivirusanwendung ist so konfiguriert, dass temporäre Internetdateien und heruntergeladene Programme durchsucht werden.	Filtern Sie Ihre Antivirusanwendung so, dass mit CA ARCserve Central Applications-Webseiten in Zusammenhang stehende Dateien aus dem Internet zugelassen werden.
Das auf Ihrem Computer installierte Skriptmodul ist fehlerhaft oder veraltet.	Aktualisieren Sie das Skriptmodul.
Die auf Ihrem Computer installierten Treiber für die Grafikkarte sind fehlerhaft oder veraltet.	Aktualisieren Sie die Treiber für die Grafikkarte.
Die auf Ihrem Computer installierte DirectX-Komponente ist fehlerhaft oder veraltet.	Aktualisieren Sie die DirectX-Komponente.

Bei der Anmeldung in CA ARCserve D2D-Knoten und -Überwachungsserver werden Webseiten nicht richtig geladen

Gültig auf Windows-Plattformen.

Symptom:

Webseiten in Browserfenstern werden nicht richtig geladen und/oder zeigen Fehlermeldungen an, wenn man sich vom Bildschirm "Knoten" aus bei CA ARCserve D2D-Knoten und -Überwachungsservern anmeldet.

Lösung:

Dieses Verhalten wirkt sich hauptsächlich auf Internet Explorer-Browser aus. Webseiten laden möglicherweise nicht richtig, wenn "Active scripting", ActiveX-Steuerelemente oder Java-Programme auf Ihrem Computer deaktiviert oder auf Ihrem Netzwerk gesperrt sind.

Sie können das Problem durch Aktualisieren Ihres Browserfensters beheben. Wenn das Aktualisieren Ihres Browserfensters das Problem jedoch nicht löst, gehen Sie wie folgt vor:

1. Öffnen Sie den Internet Explorer.

   Klicken Sie im Menü "Extras" auf "Internetoptionen".

   Das Dialogfeld "Internetoptionen" wird geöffnet.

2. Klicken Sie auf die Registerkarte "Sicherheit".

   Die Sicherheitsoptionen werden angezeigt.

3. Klicken Sie auf "Internetzone".

   Die Optionen der Internetzonen werden angezeigt.

4. Klicken Sie auf "Stufe anpassen".

   Das Dialogfeld "Sicherheitseinstellungen - Internetzone" öffnet sich.

5. Blättern Sie bis zur Kategorie "Scripting".

   Suchen Sie "Active Scripting".

   Klicken Sie auf die Option "Aktivieren" oder "Auffordern".

6. Klicken Sie in den Sicherheitseinstellungen auf das Dialogfeld "OK Internetzone".

   Das Dialogfeld "Sicherheitseinstellungen - Internetzone" wird geschlossen.

7. Klicken Sie im Dialogfeld "Internetoptionen" auf "OK".

   Das Dialogfeld "Internetoptionen" wird geschlossen und die Option "Active Scripting" wird angewendet.

Hinweis: Wenn diese Lösung das Problem nicht behebt, setzen Sie sich mit Ihrem Systemadministrator in Verbindung und stellen Sie sicher, dass andere Programme wie Antivirus- oder Firewall-Programme "Active Scripting", ActiveX-Steuerelemente oder Java-Programme nicht blockieren.

Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift.

Gültig auf allen unterstützten Windows-Betriebssystemen. Gilt für alle Browser.

Symptom:

Wenn Sie sich bei CA ARCserve Central Applications anmelden, werden Störzeichen im Inhaltsbereich Ihres Browserfensters angezeigt.

Lösung:

Dieses Problem tritt auf, wenn Sie CA ARCserve Central Applications mithilfe von HTTPS-Kommunikation installieren und dann versuchen, auf CA ARCserve Central Applications mithilfe von HTTP-Kommunikation zuzugreifen. Die zugrunde liegende Webservices-Komponente in CA ARCserve Central Applications unterstützt den Wechsel von HTTP-URLs zu HTTPS-URLs nicht. Dadurch werden Störzeichen in Ihrem Browserfenster angezeigt. Beispiel:

Um dieses Problem zu beheben, greifen Sie mithilfe von HTTPS auf CA ARCserve Central Applications zu, wenn Sie die Anwendungen installieren oder konfigurieren, um mithilfe von HTTPS zu kommunizieren.

CA ARCserve D2D-Webservice schlägt auf CA ARCserve D2D-Knoten fehl

Gültig auf Windows-Plattformen.

Symptom:

Der Webservice, der auf den CA ARCserve D2D-Knoten ausgeführt wird, startet und schlägt fehl oder kann nicht starten.

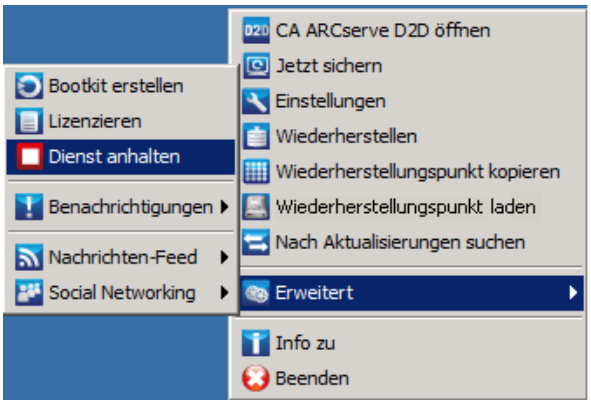
Lösung:

Dieses Problem tritt auf, wenn der vom CA ARCserve D2D-Webservice verwendete Port derselbe ist wie der Port, der vom VMware vCenter-Webservice (Tomcat) verwendet wird.

Der Port, den CA ARCserve D2D verwendet, kann mit dem Standardport von Tomcat im Konflikt stehen. Durch diesen Konflikt schlägt Tomcat fehl, wenn CA ARCserve D2D davor gestartet wird. Um dieses Problem zu beheben, können Sie den Standardport für Tomcat wie folgt ändern:

1. Klicken Sie im CA ARCserve D2D-Monitor auf die Option "Erweitert", und wählen Sie "Dienst anhalten".

   Der CA ARCserve D2D-Webdienst wird angehalten.

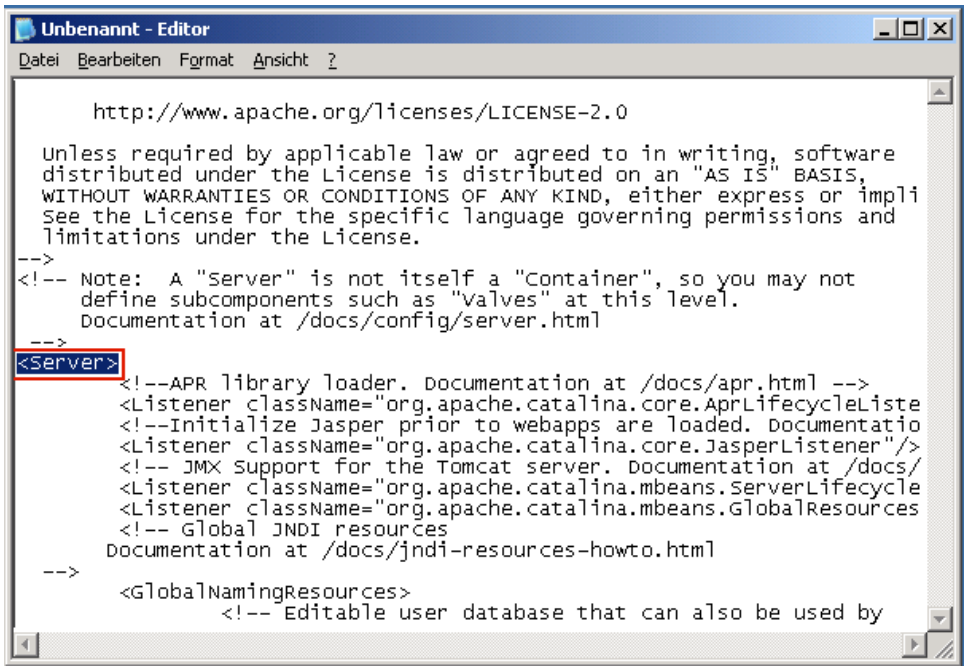
   

2. Öffnen Sie die Tomcat-Datei "server.xml", um das Verhalten von Tomcat zu bearbeiten bzw. zu konfigurieren.

   Die Tomcat-Datei "server.xml" ist unter der folgenden Ordnerstruktur zu finden:

   `C:\Programme\CA\ARCserve Central Applications\TOMCAT\conf`

3. Suchen Sie den Tag <Server> in der Datei "server.xml".



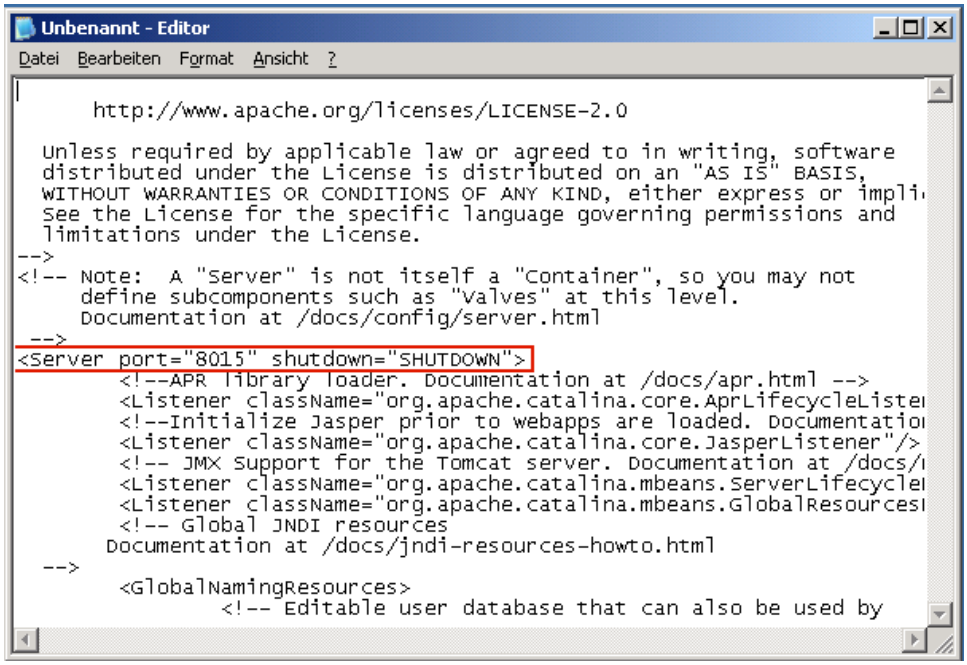
4. Bearbeiten Sie den Tag <Server> wie folgt:

   Von:

   <Server>

   In:

   <Server port="8015" shutdown="SHUTDOWN">



5. Speichern und schließen Sie die Datei "server.xml".

   Der Befehl zum Schließen von Tomcat wurde konfiguriert und kann nun vom Server auf dem genannten Port (8015) empfangen werden.

6. Klicken Sie im CA ARCserve D2D-Monitor auf die Option "Erweitert", und wählen Sie "Dienst starten".

   Der CA ARCserve D2D-Webdienst wird gestartet.

Der CA ARCserve D2D-Webservice wird nur langsam ausgeführt.

Gültig auf Windows-Betriebssystemen.

Symptom 1:

Der CA ARCserve D2D-Webservice auf CA ARCserve D2D-Systemen wird nur langsam ausgeführt. Es kann zu weiteren Symptomen kommen, wie:

- Der CA ARCserve D2D-Webservice antwortet nicht mehr oder belegt 100 Prozent der CPU-Ressourcen.
- CA ARCserve D2D-Knoten funktionieren nicht ordnungsgemäß oder können nicht mit dem Webservice kommunizieren.

Lösung 1:

In verschiedenen Umgebungskonfigurationen können Sie erkennen, dass der CA ARCserve D2D-Webservice zu viel CPU-Zeit in Anspruch nimmt oder die Reaktionszeit zu lange ist. Standardmäßig wird Tomcat konfiguriert, um den Knoten einen beschränkten Speicher zuzuweisen, der möglicherweise nicht für Ihre Umgebung geeignet sind. Um diesem Problem nachzugehen, überprüfen Sie folgende Protokolldateien:

```
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log
```

Suchen Sie die folgende Meldung:

```
java.lang.OutOfMemoryError
```

Um dieses Problem zu beheben, erhöhen Sie den zugewiesenen Speicher.

Führen Sie folgende Schritte aus, um den Speicher zu erhöhen:

1. Öffnen Sie den Registrierungs-Editor, und wählen Sie den folgenden Schlüssel aus:
   - x86-Betriebssysteme:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java
     ```

   - x64-Betriebssysteme:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java
     ```

2. Wählen Sie eine der folgenden Vorgehensweisen:

   - Wenn folgende Meldung in der Protokolldatei angezeigt wird:

     ```
     java.lang.OutOfMemoryError: PermGen space
     ```

     Hängen Sie Folgendes dem Wert der Optionen an.

     ```
     -XX:PermSize=128M -XX:MaxPermSize=128M
     ```

     Hinweis: Möglicherweise müssen Sie den Wert "-XX:MaxPermSize" erhöhen, um Ihre Umgebung anzupassen.

   - Wenn eine der folgenden Meldung in der Protokolldatei angezeigt wird:

     ```
     java.lang.OutOfMemoryError: Java heap space
     java.lang.OutOfMemoryError: GC overhead limit exceeded
     ```

     Erhöhen Sie den Wert des folgenden DWORD:

     ```
     JvmMx
     ```

3. Starten Sie den CA ARCserve D2D-Webservice neu.

Symptom 2

Geplante Sicherungen werden übersprungen und nicht mehr ausgeführt.

Lösung 2

Wenn Sie den maximalen Wert für gleichzeitige Sicherungen als 20 oder weniger konfigurieren, gehen Sie wie folgt vor:

1. Erhöhen Sie den Wert des folgenden DWORD:

   ```
   JvmMx=256
   ```

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

2. Hängen Sie Folgendes dem Wert der Optionen an.

   ```
   -XX:MaxPermSize=128M
   ```

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

Wenn Sie den maximalen Wert für gleichzeitige Sicherungen als über 20 aber unter 50 konfigurieren, gehen Sie wie folgt vor:

1. Erhöhen Sie den Wert des folgenden DWORD:

   ```
   JvmMx=512
   ```

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

2. Hängen Sie Folgendes dem Wert der Optionen an.

   ```
   -XX:MaxPermSize=256M
   ```

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

CA ARCserve Central Virtual Standby kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen.

Gültig auf Windows-Betriebssystemen.

Symptom:

CA ARCserve Central Virtual Standby kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen.

Lösung:

In der folgenden Tabelle wird beschrieben, warum CA ARCserve Central Virtual Standby keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen kann, und enthält entsprechende Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Das Netzwerk war bei der Anwendung der Richtlinien nicht verfügbar oder stabil.	Stellen Sie sicher, dass das Netzwerk verfügbar und stabil ist, und versuchen Sie es dann erneut.
Der CA ARCserve D2D-Computer könnte die Arbeitslast nicht verarbeiten, als die Anwendung versuchte, mit dem Knoten zu kommunizieren.	Stellen Sie sicher, dass der CPU auf dem CA ARCserve D2D-Remote-Knoten in einem Normalzustand ist, und versuchen Sie es dann erneut.
Der CA ARCserve D2D-Dienst auf dem Remote-Knoten wurde bei der Anwendung der Richtlinien nicht ausgeführt.	Stellen Sie sicher, dass CA ARCserve D2D auf dem Remote-Knoten ausgeführt wird, und versuchen Sie es dann erneut.
Die Kommunikation des CA ARCserve D2D-Diensts funktionierte nicht richtig.	Starten Sie den CA ARCserve D2D-Dienst auf dem Remote-Knoten neu, und versuchen Sie es dann erneut.

Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt.

Gültig auf Windows-Plattformen.

Symptom:

Die folgende Meldung wird in Ihrem Browserfenster angezeigt, wenn Sie sich bei der Anwendung anmelden:

- Internet Explorer:

  `Es gibt ein Problem mit dem Sicherheitszertifikat dieser Website.`

- Firefox:

  `Diese Verbindung ist nicht vertrauenswürdig.`

- Chrome:

  `Dem Sicherheitszertifikat dieser Seite wird nicht vertraut!`

Wenn Sie eine Option angeben, mit der Sie zur Website gelangen, können Sie erfolgreich bei der Anwendung anmelden. Dieses Verhalten tritt jedoch jedes Mal auf, wenn Sie sich bei der Anwendung anmelden.

Lösung:

Dieses Verhalten tritt auf, wenn Sie angeben, dass HTTPS als Kommunikationsprotokoll verwendet werden soll. Um dieses Problem vorübergehend zu korrigieren, klicken Sie in Ihrem Browserfenster auf den Link, mit dem Sie weiter zur Website gelangen. Diese Meldung wird jedoch jedes Mal angezeigt werden, wenn Sie sich bei der Anwendung anmelden.

Das HTTPS-Kommunikationsprotokoll bietet eine höhere Sicherheitsebene als das HTTP-Kommunikationsprotokoll. Wenn Sie weiterhin unter Verwendung eines HTTPS-Kommunikationsprotokolls kommunizieren möchten, können Sie ein Sicherheitszertifikat von VeriSign erwerben und das Zertifikat auf dem Anwendungsserver installieren. Optional können Sie das von der Anwendung verwendete Kommunikationsprotokoll in HTTP ändern. Um das Kommunikationsprotokoll in HTTP zu ändern, gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, auf dem Sie die Anwendung installiert haben.
2. Wechseln Sie zu dem folgenden Verzeichnis:

   `C:\Programme\CA\ARCserve Central Applications\BIN`
3. Führen Sie die folgende Batch-Datei aus:

   `ChangeToHttp.bat`
4. Nachdem die Batch-Datei ausgeführt wurde, öffnen Sie Windows Server Manager.

   Starten Sie den folgenden Dienst neu:

   `CA ARCserve Central Applications Service`

Beim Hinzufügen von Knoten werden ungültige Anmeldeinformationen angezeigt.

Gültig auf Windows-Plattformen.

Symptom:

Die folgende Meldung wird angezeigt, wenn Sie versuchen, zum Bildschirm "Knoten" Knoten hinzuzufügen:

`Ungültige Anmeldeinformationen.`

Lösung:

Dieses Problem tritt in den folgenden Szenarien auf:

- Die angegebenen Anmeldeinformationen im Dialogfeld "Knoten hinzufügen" sind falsch.
- Die Uhrzeit auf dem Knoten ist nicht die gleiche wie auf dem Anwendungsserver.

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Anwendungsserver und dann bei der Anwendung an.
2. Klicken Sie auf der Startseite in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt:

3. Klicken Sie in der Symbolleiste "Knoten" auf "Hinzufügen", und dann im Pop-up-Menü auf "Knoten nach IP/Namen hinzufügen".

   Das Dialogfeld "Knoten nach IP/Namen hinzufügen" wird geöffnet.

4. Füllen Sie folgende Felder im Dialogfeld "Knoten nach IP/Namen hinzufügen" aus:

   - **IP/Knotenname:** Lässt Sie die IP-Adresse oder den Namen des Knotens festlegen.
   - **Beschreibung:** Lässt Sie eine Beschreibung für den Knoten festlegen.
   - **Benutzername:** Lässt Sie den Windows-Benutzernamen festlegen, der für die Anmeldung beim Knoten erforderlich ist.
   - **Kennwort:** Lässt Sie das Kennwort festlegen, das für die Anmeldung beim Knoten erforderlich ist.

   Klicken Sie auf "Validieren".

5. Wenn die Meldung "Ungültige Anmeldeinformationen" angezeigt wird, gehen Sie wie folgt vor:

   a. Stellen Sie sicher, dass Sie auf dem Dialogfeld "Knoten hinzufügen" die richtigen Anmeldeinformationen angegeben haben und klicken Sie dann auf "Bestätigen".

   b. Wenn die Meldung "Ungültige Anmeldeinformationen" angezeigt wird, stellen Sie sicher, dass die Uhrzeit des Betriebssystems auf dem Anwendungsserver die gleiche ist wie die des Betriebssystems auf dem Knoten.

      Hinweis: Die Uhrzeiten der Betriebssysteme können sich in verschiedenen Zeitzonen befinden. Die Uhrzeiten der Betriebssysteme können nicht unterschiedliche Daten haben. Stellen Sie vor allem sicher, dass das Datum des Betriebssystems auf dem Knoten sich nicht um mehr als einen Kalendertag von dem Datum des Betriebssystems auf dem Anwendungsserver unterscheidet.

Meldungen zu ungültigen Anmeldeinformationen unter Windows XP

Gültig auf Computern mit Windows XP-Betriebssystemen.

Symptom:

Wenn Sie Windows XP-basierte Knoten im Bildschirm "Knoten" hinzufügen, wird die folgende Meldung angezeigt:

```
Ungültige Benutzeranmeldeinformationen.
```

Lösung:

Unter verschiedenen Bedingungen kann CA ARCserve Central Virtual Standby keine Windows XP-basierten Knoten hinzufügen, für die "Ordneroptionen" unter "Windows" > "Einfache Dateifreigabe verwenden" aktiviert wurde. Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows XP-Knoten an und öffnen Sie den Windows Explorer.
2. Klicken Sie im Menü "Extras" auf "Ordneroptionen".

   Das Dialogfeld "Ordneroptionen" wird geöffnet.
3. Klicken Sie auf "Anzeigen", und blättern Sie weiter zu "Einfache Dateifreigabe verwenden (empfohlen)".
4. Deaktivieren Sie das Kontrollkästchen neben "Einfache Dateifreigabe verwenden (empfohlen)", und klicken Sie auf "OK".

   Die einfache Dateifreigabe ist nun deaktiviert.
5. Melden Sie sich beim CA ARCserve Central Virtual Standby-Server an, und fügen Sie anschließend den Knoten hinzu.

Fehler wegen verweigerten Zugriffs beim Hinzufügen eines Knotens nach IP/Namen

Gültig für alle Windows-Betriebssysteme, die Benutzerkontensteuerung (User Access Control, UAC) unterstützen.

Hinweis: Windows Vista, Windows Server 2008, Windows Server 2008 R2 und Windows 7 unterstützen UAC.

Symptom:

Wenn Sie Knoten über das Dialogfeld "Knoten nach IP/Namen hinzufügen" mithilfe eines neuen Windows-Benutzerkontos hinzufügen, das ein Mitglied der Administratorgruppe ist, wird folgende Meldung angezeigt:

```
Zugriff verweigert. Stellen Sie sicher, dass der Benutzer Administratorrechte hat und der Remote-Registrierungszugriff nicht durch eine lokale Sicherheitsrichtlinie des hinzugefügten Rechners beschränkt ist.
```

Das Ergebnis ist, dass Sie den Knoten nicht hinzufügen können.

Lösung:

Sie können dieses Verhalten erwarten, wenn UAC auf Computern aktiviert ist, auf denen ein Windows-Betriebssystem ausgeführt wird, das UAC unterstützt. UAC ist eine Windows-Funktion, durch die es ausschließlich dem Administratorkonto ermöglicht wird, sich von einem Remote-Standort an dem Computer anzumelden. Die Lösung für dieses Verhalten besteht in den folgenden Schritten:

Gehen Sie wie folgt vor:

1. Melden Sie sich über das Administratorkonto beim Knoten an.
2. Öffnen Sie die Windows-Systemsteuerung.
3. Öffnen Sie die Benutzerkonten.
4. Klicken Sie im Fenster "Änderungen am eigenen Konto durchführen" auf "Einstellungen der Benutzerkontensteuerung ändern", und führen Sie anschließend einen der folgenden Schritte durch:

   - **Windows Vista und Windows Server 2008:** Klicken Sie im Fenster "Änderungen am eigenen Konto durchführen" auf "Benutzerkontensteuerung ein- oder ausschalten" Deaktivieren Sie anschließend im Fenster "Benutzerkontensteuerung einschalten, um den Computer sicherer zu machen" das Kontrollkästchen neben "Benutzerkontensteuerung verwenden, um zum Schutz des Computers beizutragen", und klicken Sie auf "OK".

     Starten Sie Ihren Computer neu, um die Änderungen auf UAC anzuwenden.

   - **Windows Server 2008 r2 und Windows 7:** Schieben Sie im Fenster "Benachrichtigungen über Änderungen an dem Computer auswählen" den Regler von "Immer benachrichtigen" auf "Nie benachrichtigen". Klicken Sie auf OK und schließen Sie die Windows-Systemsteuerung.

     Starten Sie Ihren Computer neu, um die Änderungen auf UAC anzuwenden.

5. Nachdem der Computer neu gestartet wurde, stellen Sie sicher, dass die folgenden Konfigurationen auf den Überwachungsserver und den CA ARCserve D2D-Knoten bzw. das Sicherungs-Proxy-System angewendet werden:
   - Der Windows-Server-Dienst wird ausgeführt.
   - Der Datei- und Druckerfreigabedienst darf durch die Windows-Firewall hindurch kommunizieren.
   - Wenn vom Knoten nicht verlangt wird, dass er sich einer Domäne anschließt, darf der Anmeldedienst durch die Windows-Firewall hindurch kommunizieren.
   - Der Wert für "Lokale Sicherheitsrichtlinie", "Lokale Richtlinien", "Sicherheitsoptionen", "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten" ist "Klassisch".
6. Vergewissern Sie sich, dass die folgende Konfiguration auf den Virtual Standby-Server angewandt wird:
   - Der Wert für "Lokale Sicherheitsrichtlinie", "Lokale Richtlinien", "Sicherheitsoptionen", "Netzwerksicherheit: LAN Manager-Authentifizierungsebene" ist "LM- und NTLM-Antworten senden (NTLMv2-Sitzungssicherheit verwenden, wenn ausgehandelt)".

Knoten werden nach einer Namensänderung nicht mehr im Bildschirm "Knoten" angezeigt

Gültig auf Windows-Plattformen.

Symptom:

Der Hostname des Knotens wurde geändert, nachdem er zum Fenster "Knoten" hinzugefügt wurde. Der Knoten wird nicht mehr im Fenster "Knoten" angezeigt.

Lösung:

Dieses Verhalten ist normal. CA ARCserve Central Virtual Standby behält den Namen des Knotens, der über das Knotenfenster hinzugefügt wurde. Wenn Sie den Knoten umbenennen, kann Virtual Standby den Knoten nicht entdecken. Der Knoten wird nicht im Fenster "Knoten" angezeigt.

Um umbenannte Knoten im Fenster "Knoten" anzuzeigen, gehen Sie folgendermaßen vor:

1. Benennen Sie den Knoten um.
2. Öffnen Sie den Bildschirm "Knoten" und löschen Sie den Knoten (siehe Seite 52), der umbenannt wurde.
3. Fügen Sie den Knoten (siehe Seite 28) unter Verwendung des neuen Namens hinzu.

Fehler "Operating System Not Found" treten auf

Gültig auf Windows-Plattformen.

Symptom:

Die folgende Meldung wird angezeigt, wenn das Einschalten des Virtual Standby-Rechners fehlschlägt:

```
Operating System Not Found (Betriebssystem nicht gefunden)
```

Lösung:

Das oben aufgeführte Verhalten kann auf virtuellen Rechner auftreten, die SCSI- und IDE-Geräte enthalten. Wenn dieses Problem auftritt, überprüfen Sie, wie die Datenträger auf Ihrem virtuellen Rechner konfiguriert sind, und stellen Sie sicher, dass die Startsequenz des wiederhergestellten virtuellen Rechners dieselbe ist, wie die der Quelle des virtuellen Rechners. Wenn die Startsequenz anders ist, aktualisieren Sie das BIOS auf dem wiederhergestellten virtuellen Rechner, damit sie mit der Startsequenz der Quelle übereinstimmt.

Hinweis: Verwenden Sie für die Darstellung des ersten IDE-Datenträgers (0:1).

Virtual Standby-Jobs an Hyper-V-Systeme schlagen fehl

Gültig auf Windows-Betriebssystemen.

Symptom:

Virtual Standby-Jobs an Hyper-V-Systeme schlagen fehl. Folgende Meldung wird im Aktivitätsprotokoll angezeigt:

```
Der Virtual Standby-Job konnte die Hyper-V-VM nicht abrufen.
```

Lösung:

Virtual Standby-Jobs schlagen unter den folgenden Bedingungen fehl:

- Der Virtual Standby-Webservice kann aus dem Hyper-V-System keine Informationen zu den virtuellen Rechnern abzurufen. Kommunikationsprobleme zwischen dem CA ARCserve Central Virtual Standby-Server und dem Hyper-V-System treten auf, wenn die erforderlichen Hyper-V-Dienste nicht im Hyper-V-System ausgeführt werden.

  Lösung: Stellen Sie sicher, dass der alle erforderlichen Hyper-V-Dienste auf dem Hyper-V-System ausgeführt werden.

- Das Hyper-V-System enthält nicht den freien Speicherplatz, der für das Erstellen des virtuellen Virtual Standby-Rechners oder zum Erstellen eines Snapshot des virtuellen Virtual Standby-Rechners benötigt wird.

  Lösung: Konfigurieren Sie das Hyper-V-System neu, um mehr freien Festplattenspeicher im Systemvolume zu schaffen.

Hinweis: Wenn Sie andere mögliche Ursachen entdecken, setzen Sie sich mit CA Support in Verbindung.

Virtual Standby-Jobs schlagen aufgrund interner Fehler fehl

Gültig auf Windows-Betriebssystemen.

Symptom 1:

Virtual Standby-Jobs schlagen fehl. Es wird eine der folgenden Meldungen im Aktivitätsprotokoll angezeigt:

```
Fehler beim Konvertieren des virtuellen Datenträgers.
Ein interner Fehler ist aufgetreten. Setzen Sie sich mit CA Support in Verbindung.
```

Außerdem wird im VDDK die folgende Fehlermeldung angezeigt:

```
Unbekannter Fehler.
```

Lösung 1:

Um dieses Problem zu beheben, beachten Sie folgende Lösungsmöglichkeiten:

- Konvertierungsvorgänge können fehlschlagen, wenn im Datenspeicher, der in der Virtual Standby-Richtlinie angegeben ist, nicht genügend freier Speicherplatz vorhanden ist. VDDK gibt die Meldung zurück, da die VDDK-API es (derzeit) nicht unterstützt, die Größe des freien Speicherplatzes im Datenspeicher zu erkennen. Um dieses Problem zu beheben, machen Sie im ursprünglichen Datenspeicher so viel Festplattenspeicher frei, wie für den Abschluss des Vorgang erforderlich ist, und übergeben Sie den Job erneut.
- Netzwerkstörungen und starker Netzwerkverkehr können dazu führen, dass die Konvertierung fehlschlägt. Um dieses Problem zu beheben, stellen Sie sicher, dass der Quellknoten über das Netzwerk mit dem ESX Server- bzw. vCenter-System kommunizieren kann, und übergeben Sie den Job erneut.
- Wenn mehrere gleichzeitige Verbindungen vorliegen, die aus Jobs zur Sicherung oder Wiederherstellung von virtuellen Rechnern auf dem ESX Server- oder vCenter Server-System bestehen - wobei Verbindungen über den VMware vSphere Client stattfinden - schlagen diese Jobs möglicherweise fehl. Um dieses Problem zu beheben, beenden Sie alle unnötigen Verbindungen, und übergeben Sie den Job erneut.

  Dieses Problem hat seine Ursache in einer Verbindungsbeschränkung in VMware-VDDK. Folgende Protokollbeschränkungen der Netzwerkdateikopie (NFC) gelten für:

  - ESX 4: maximal 9 Direktverbindungen
  - ESX 4 über vCenter-Server: maximal 27 Verbindungen
  - ESXi 4: maximal 11 Direktverbindungen
  - ESXi 4 über vCenter-Server: maximal 23 Verbindungen
  - ESXi 5: Von einem Übertragungspuffer für alle NFC-Verbindungen beschränkt und vom Host erzwungen; die Summe aller NFC-Verbindungpuffer zu einem ESXi-Host kann 32 MB nicht überschreiten. 52 Verbindungen durch vCenter Server einschließlich der Grenze pro Host.

  Hinweis: Verbindungen können nicht über Festplatten hinweg gemeinsam genutzt werden. Die Werte für "Maximale Beschränkungen" beziehen sich nicht auf SAN- und Hotadd-Verbindungen. Wenn der NFC-Client nicht ordnungsgemäß heruntergefahren wird, können Verbindungen für zehn Minuten offen bleiben.
- Prüfen Sie die Abschnitte "Tasks" (Aufgaben) und "Events" (Ereignisse) des VMware vSphere Client-Protokolls, um interne Fehler beim spezifischen virtuellen Rechner zu entdecken. Beheben Sie die internen Fehler, und übergeben Sie den Job erneut.

  Beispiel: Eine andere Anwendung bzw. ein anderer Vorgang verwendet die VMDK-Datei. Um dieses Problem zu beheben, geben Sie die Datei frei, und übergeben Sie den Job erneut.

Symptom 2:

Virtual Standby-Jobs schlagen fehl. Es wird eine der folgenden Meldungen im Aktivitätsprotokoll angezeigt:

```
Fehler beim Konvertieren des virtuellen Datenträgers.
Ein interner Fehler ist aufgetreten. Setzen Sie sich mit CA Support in Verbindung.
```

Außerdem wird im VDDK die folgende Fehlermeldung angezeigt:

```
Open vmdk failed with error File not found. (Öffnen von vmdk fehlgeschlagen, Datei nicht gefunden)
```

Lösung 2:

Dieses Problem kann unter den folgenden Bedingungen auftreten:

- In VDDK wurde ein Snapshot nicht richtig bearbeitet.
- In VDDK wurde ein Snapshot nicht manuell oder nicht vom virtuellen Rechner entfernt.

Um dieses Problem zu beheben, übergeben Sie den Job erneut. Wenn der Job erneut fehlschlägt, löschen Sie den wiederhergestellten virtuellen Rechner, und übergeben Sie den Job erneut.

Symptom 3:

Virtual Standby-Jobs schlagen fehl. Es wird eine der folgenden Meldungen im Aktivitätsprotokoll angezeigt:

```
Fehler beim Konvertieren des virtuellen Datenträgers.
Ein interner Fehler ist aufgetreten. Setzen Sie sich mit CA Support in Verbindung.
```

Außerdem wird im VDDK die folgende Fehlermeldung angezeigt:

```
Open vmdk failed or "The server refused connection" error message
```

Lösung 3:

Dieses Problem hat seine Ursache in einer Verbindungsbeschränkung in VMware-VDDK. Folgende Protokollbeschränkungen der Netzwerkdateikopie (NFC) gelten für:

- ESX 4: maximal 9 Direktverbindungen
- ESX 4 über vCenter-Server: maximal 27 Verbindungen
- ESXi 4: maximal 11 Direktverbindungen
- ESXi 4 über vCenter-Server: maximal 23 Verbindungen

Hinweis: Verbindungen können nicht über Festplatten hinweg gemeinsam genutzt werden. Die Werte für "Maximale Beschränkungen" beziehen sich nicht auf SAN- und Hotadd-Verbindungen. Wenn der NFC-Client nicht ordnungsgemäß heruntergefahren wird, können Verbindungen für zehn Minuten offen bleiben.

Virtual Standby-Jobs im Hotadd-Transportmodus schlagen fehl

Gültig auf Windows-Plattformen.

Symptom:

Wiederherstellungsvorgänge schlagen fehl, wenn Daten im Hotadd-Transportmodus wiederhergestellt werden. Folgende Meldung wird im Aktivitätsprotokoll angezeigt:

```
Es ist ein unerwarteter Fehler aufgetreten. Wenden Sie sich an den technischen Support.
```

Außerdem wird im VDDK die folgende Fehlermeldung angezeigt:

```
Unbekannter Fehler.
```

Lösung:

Wiederherstellungsvorgänge schlagen im Hotadd-Transportmodus fehl, wenn die Datenträgereinstellungen nicht ordnungsgemäß konfiguriert sind.

Zum Konfigurieren des Datenträgers gehen Sie wie folgt vor:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxysystems an.

   Öffnen Sie die Windows-Befehlszeile.

2. Geben Sie in der Befehlszeile folgenden Befehl ein:

   ```
   diskpart
   ```

   Drücken Sie die Eingabetaste.

   Gaben Sie "SAN" ein, und drücken Sie die Eingabetaste.

   Die aktuellen SAN-Richtlinie wird angezeigt.

3. Geben Sie folgenden Befehl ein:

   ```
   SAN POLICY = OnlineAll
   ```

   Drücken Sie die Eingabetaste.

   Die SAN-Richtlinie wird so konfiguriert, dass SAN-gehostete Volumes nicht automatisch geladen werden.

4. Um das schreibgeschützte Attribut des spezifischen SAN-Datenträgers zu löschen, wählen Sie den Datenträger aus der Datenträgerliste aus, und geben Sie den folgenden Befehl ein:

   ```
   attribute disk clear readonly
   ```

   Drücken Sie die Eingabetaste.

5. Gaben Sie "exit" ein, und drücken Sie die Eingabetaste.

Der Datenträger ist nun konfiguriert, und Sie können den Job erneut übergeben. Wenn der Job erneut fehlschlägt, laden Sie die Hotadd-Datenträger über die Datenträgerverwaltung des Proxysystems.

Um die Datenträger manuell zu laden, gehen Sie wie folgt vor:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxysystems an.

   Öffnen Sie Windows-Systemsteuerung, und doppelklicken Sie auf "Verwaltung".

   Das Fenster "Verwaltung" wird geöffnet.

2. Doppelklicken Sie in der Liste "Favoriten" auf "Computerverwaltung".

   "Computerverwaltung" wird geöffnet.

3. Erweitern Sie den Bereich "Speicherung", und klicken Sie auf "Datenträgerverwaltung".

   Die Datenträger werden angezeigt.

4. Klicken Sie mit der rechten Maustaste auf den zu entfernenden Datenträger, und klicken Sie auf "Online".

   Der Datenträger ist nun geladen, und Sie können den Job erneut übergeben.

Virtual Standby-Jobs enden Mit Warnmeldungen zu fehlenden Sitzungen

Gültig auf Windows-Plattformen.

Symptom:

Die Virtual Standby-Jobs enden, und eine der folgenden Meldungen wird im Aktivitätsprotokoll angezeigt:

```
Der Virtual Standby-Job endet ohne Sitzung(en).
```

```
Virtual Standby konnte keine Sicherungssitzungen auf dem CA ARCserve D2D-Server erkennen, um Wiederherstellungspunkt-Snapshots zu erstellen. Möglicherweise sind auf dem CA ARCserve D2D-Server keine Sicherungssitzungen vorhanden, die konvertiert werden können.
```

Lösung:

Probleme dieser Art treten unter den folgenden Bedingungen auf:

- Sie haben CA ARCserve Central Protection Manager verwendet, um die CA ARCserve D2D-Sicherungsrichtlinie auf den Knoten anzuwenden, und es ist einer der nachstehend beschriebenen Fälle eingetreten.
  - Die Einstellungen der CA ARCserve D2D-Sicherungsquelle wurden von "Einzelne Volumes zur Sicherung auswählen" in "Gesamten Rechner sichern" umgeändert, und es wurde keine vollständige Sicherung übergeben oder abgeschlossen, die die durch Bereitstellung der Virtual Standby-Richtlinie aktualisierten Sicherungseinstellungen enthält.

    Lösung: Übergeben Sie eine vollständige Sicherung des CA ARCserve D2D-Knotens.
  - Die Einstellungen der CA ARCserve D2D-Sicherungsquelle wurden von "Gesamten Rechner sichern" in "Einzelne Volumes zur Sicherung auswählen" umgeändert, nachdem die Virtual Standby-Richtlinie für den Knoten bereitgestellt wurde.

    Lösung: Ändern Sie die Einstellungen der CA ARCserve D2D-Sicherungsquelle von "Einzelne Volumes zur Sicherung auswählen" in "Gesamten Rechner sichern" um, und übergeben Sie anschließend eine vollständige Sicherung des CA ARCserve D2D-Knotens.

Sicherungs- und Wiederherstellungsjobs verwenden den SAN-Transportmodus nicht

Gültig auf Windows-Plattformen.

Symptom:

Sicherungs- und Wiederherstellungsjobs verwenden den SAN-Transportmodus (siehe Seite 225) nicht. Die Jobs werden auf den zum NBD-Transportmodus (siehe Seite 225) oder den NBDSSL-Transportmodus (siehe Seite 225) zurückgesetzt. Der verwendete Modus wird im Feld "Transportmodus" im Dialogfeld "Statusüberwachung der Sicherung" angezeigt.

Lösung:

Die oben beschriebenen Symptome können auftreten, wenn die SAN-LUN im Sicherungs-Proxysystem nicht richtig konfiguriert ist. Wenn Windows-Datenträgerverwaltung die SAN-LUN entdeckt und das Problem weiter besteht, ist der Datenträger möglicherweise offline, oder das Leseattribut für den Datenträger ist nicht richtig. Um dieses Verhalten zu vermeiden, konfigurieren Sie den Datenträger neu.

Zum Konfigurieren des Datenträgers gehen Sie wie folgt vor:

1. Melden Sie sich mithilfe eines Kontos mit administrativen Berechtigungen beim Quellknoten oder Überwachungsserver an.
2. Öffnen Sie die Windows-Befehlszeile.
3. Geben Sie in der Befehlszeile folgenden Befehl ein:

   ```
   diskpart
   ```

   Drücken Sie die Eingabetaste.
4. Gaben Sie "SAN" ein, und drücken Sie die Eingabetaste.

   Die aktuellen SAN-Richtlinie wird angezeigt.
5. Geben Sie folgenden Befehl ein:

   ```
   SAN POLICY = OnlineAll
   ```

   Drücken Sie die Eingabetaste.

   Die SAN-Richtlinie wird so konfiguriert, dass SAN-gehostete Volumes nicht automatisch geladen werden.
6. Um das schreibgeschützte Attribut des spezifischen SAN-Datenträgers zu löschen, wählen Sie den Datenträger aus der Datenträgerliste aus, und geben Sie den folgenden Befehl ein:

   ```
   attribute disk clear readonly
   ```

   Drücken Sie die Eingabetaste.
7. Gaben Sie "exit" ein, und drücken Sie die Eingabetaste.

Der Datenträger ist nun konfiguriert, und Sie können den Job erneut übergeben.

Bei Sicherungen und Wiederherstellungen im Hotadd-Transportmodus werden Datenträger nicht geladen

Gültig auf Windows-Plattformen.

Symptom:

Bei Sicherungs- und Wiederherstellungsjobs im Hotadd-Transportmodus können Datenträger nicht im Quellknoten oder Überwachungsserver geladen werden. Zusätzlich wird im Aktivitätsprotokoll die folgende Meldung angezeigt:

```
VMDK-Datei %1!s! konnte nicht geöffnet werden. Weitere Informationen finden Sie im
Debug-Protokoll 'AFBackend.Log'.  Wenden Sie sich an den technischen Support.
```

Lösung:

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Öffnen Sie VMware vSphere Client.

   Melden Sie sich mit administrativen Anmeldeinformationen beim ESX Server-System an.

2. Wählen Sie den virtuellen Proxy-Rechner aus, und bearbeiten Sie seine Einstellungen.

3. Entfernen Sie die Hotadd-Datenträger aus dem Proxy-System, wenn während des Konvertierungsjobs Datenträger angehängt wurden.

4. Übergeben Sie den Job erneut.

Fehlernummern der Fehlerbehebung

Folgende Tabelle bezeichnet Fehlernummern als Pop-Up-Meldungen, wenn Knoten mithilfe von CA ARCserve Central Virtual Standby hinzufügt oder aktualisiert werden.

Fehlernummer	Beschreibung	Lösungsvorschlag
12884901933	Es kann keine Verbindung zum CA ARCserve D2D-Dienst auf *** hergestellt werden, und die Fehlernummer ist 12884901933. Stellen Sie sicher, dass alle Eingaben für den Knoten ist richtig sind und der CA ARCserve D2D-Dienst ausgeführt wird.	Überprüfen Sie Folgendes: ■ Der CA ARCserve D2D-Dienst wird auf dem Knoten ausgeführt. ■ Der Hostname, die IP-Adresse und das Übertragungsprotokoll, die für den Knoten angegeben wurden, sind richtig. ■ Der CA ARCserve D2D-Webservice auf dem Knoten wird ausgeführt und ist nicht gesperrt, da DNS die IP-Adresse nicht für den Knoten auflösen kann. ■ Der CA ARCserve D2D-Webservice auf dem Knoten wird ausgeführt und die Windows-Firewall, oder eine andere Firewall, sperrt nicht die Kommunikation. ■ Das Netzwerkkabel, das mit dem Knoten verbunden ist, funktioniert ordnungsgemäß. ■ Der auf dem Knoten angemeldete Benutzer erhält die erforderlichen Berechtigungen, um über ein drahtloses Netzwerk zu kommunizieren.

Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet

Gültig für Windows

Symptom:

Wenn ich eine neue Registerkartenverknüpfung unter Angabe einer HTTPS-URL hinzufüge, wird folgende Fehlermeldung angezeigt, wenn ich auf die neue Registerkarte klicke:

- Internet Explorer 8 oder 9:

  ```
  Der Inhalt wurde geblockt, da er nicht mit einem gültigen Sicherheitszertifikat signiert wurde.
  ```

- Chrome:

  ```
  The webpage is not available.
  ```

Lösung:

Um dieses Problem für Internet Explorer zu beheben, gehen Sie folgendermaßen vor:

- Internet Explorer 8

  Klicken Sie auf die Statusleiste, und aktivieren Sie "Geblockte Inhalte anzeigen".

- Internet Explorer 9

  Klicken Sie auf der Statusleiste im unteren Bereich der Seite auf die Schaltfläche "Inhalt einblenden". Die Seite wird aktualisiert, und die hinzugefügte Registerkartenverknüpfung funktioniert.

Um dieses Problem für Chrome zu beheben, gehen Sie folgendermaßen vor:

Schritt 1 - Zertifikat exportieren:

1. Öffnen Sie eine neue Registerkarte in Chrome, und geben Sie die HTTPS-URL ein.

   Folgende Warnmeldung wird angezeigt: "Das Sicherheitszertifikat der Website ist nicht vertrauenswürdig!"

2. Klicken Sie im Adressbalken auf das mit einem "X" versehene Schlosssymbol.

   Ein Pop-up-Fenster mit einer Verknüpfung namens "Zertifikatinformationen" wird geöffnet.

3. Klicken Sie auf die Verknüpfung "Zertifikatinformationen".

   Das Dialogfeld "Certificate" wird geöffnet.

4. Klicken Sie auf die Registerkarte "Details"und anschließend auf "Copy to File", um das Zertifikat auf Ihrem lokalen Computer zu speichern.

   Das Dialogfeld "Certificate Export Wizard" wird geöffnet.

5. Klicken Sie auf "Next", um das Format auszuwählen, das Sie verwenden möchten, um die Datei zu exportieren.

   Hinweis: Standardmäßig ist DER encoded binary X.509 (.CER) aktiviert.

6. Klicken Sie auf "Next", um nach einem Speicherort zu suchen, an dem Sie das Zertifikat speichern möchten.

7. Klicken Sie auf "Next", um den Zertifikatsexport-Assistenten abzuschließen, und anschließend auf "Finish".

Das Zertifikat ist nun erfolgreich exportiert.

Schritt 2 - Zertifikat importieren:

1. Öffnen Sie die Tools-Optionen von Chrome.

   Das Dialogfeld "Options" wird geöffnet.

2. Wählen Sie die Option "Details", und klicken Sie neben "HTTPS/SSL" auf Zertifikate verwalten".

   Das Dialogfeld "Certificates" wird geöffnet.

3. Klicken Sie auf "Import".

   Das Dialogfeld "Certificate Import Wizard" wird geöffnet.

4. Klicken Sie auf "Next", um nach dem Zertifikat zu suchen, das Sie auf Ihrem lokalen Computer gespeichert haben.

5. Klicken Sie auf "Next", um den Zertifikatspeicher ("Certificate Store") zu öffnen.

   Das Dialogfeld "Certificate Store" wird geöffnet.

6. Klicken Sie auf "Browse", um das Dialogfeld "Select Certificate Store" zu öffnen.

   Das Dialogfeld "Select Certificate Store" wird angezeigt:

7. Wählen Sie in der Dateiliste "Trusted Root Certification Authorities", und klicken Sie auf "OK".

   Das Dialogfeld "Certificate Store" wird angezeigt:

8. Klicken Sie auf "Next", um den Zertifikatsimport-Assistenten abzuschließen, und anschließend auf "Finish".

   Es wird eine Sicherheitswarnung angezeigt, die Sie informiert, dass Sie gerade ein Zertifikat installieren.

   Klicken Sie auf "Yes", um den Bedingungen zuzustimmen.

Die Zertifikat wurde erfolgreich importiert.

Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer 8 und 9 nicht ordnungsgemäß geöffnet

Gültig für Windows

Symptom:

Für eine HTTPS-URL einer CA ARCserve Central Applications-Anwendung:

Wenn ich eine neue Registerkartenverknüpfung unter Angabe einer HTTPS-URL zur Navigationsleiste hinzufüge, wird folgende Fehlermeldung angezeigt, wenn ich auf die neue Registerkarte und die Verknüpfung "Feedback" klicke:

```
Die Navigation zu der Webseite wurde abgebrochen.
```

Außerdem werden die RSS-Feeds nicht angezeigt.

Hinweis: Die Verknüpfung "Feedback" zeigt die Fehlermeldung auch dann an, wenn Sie die neu hinzugefügte Registerkartenverknüpfung nicht auswählen.

Lösung:

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

- Internet Explorer 8

  Nachdem Sie sich angemeldet haben, klicken Sie in der Pop-up-Sicherheitswarnmeldung "Möchten Sie nur die Webseiteninhalte anzeigen, die über eine sichere Verbindung übermittelt wurden?" auf "Nein". Dadurch erlauben Sie ungesicherte Inhalte für Ihre Website.

- Internet Explorer 9

  Klicken Sie auf der Statusleiste im unteren Bereich der Seite auf die Schaltfläche "Gesamten Inhalt anzeigen". Die Seite wird aktualisiert, und die hinzugefügte Registerkartenverknüpfung funktioniert.

Bei der Verwendung einer japanischen Tastatur können in Filterfeldern keine Sternchen und Unterstriche als ein Platzhalter verwendet werden

Gültig für Windows

Symptom:

Aufgrund der unterschiedlichen Tastencodes auf US- und japanischen Tastaturen können Sie mit japanischen Tastaturen das Platzhalterzeichen (*) und andere Sonderzeichen wie z. B. Unterstriche (_) nicht in die folgenden Filterfelder eingeben:

- Dies tritt nur in Firefox ein:
  - Knoten > Gruppe hinzufügen - Feld "Knotennamenfilter"
  - Richtlinien >-Registerkarte "Richtlinienzuweisung" > Richtlinie Zuweisen und Zuweisung aufheben - Feld "Knotennamenfilter"
  - Wiederherstellung > Knoten-Explorer - Feld "Knotenname"

Lösung:

- Um dies zu vermeiden, öffnen Sie ein Textbearbeitungsprogramm wie Notepad. Geben Sie die Sonderzeichen("*", "_" usw.) im Texteditor ein. Kopieren Sie die Zeichen anschließend aus dem Texteditor in das Feld.

Virtuelle Rechner nicht automatisch eingeschaltet

Gültig für Windows

Symptom:

Virtuelle Rechner werden nicht automatisch eingeschaltet. Der Wert von "Wiederherstellung", "Aushilfseinstellungen" ist auf "Virtuellen Rechner automatisch starten" eingestellt.

Lösung:

Hierbei handelt es sich um ein erwartetes Verhalten. Die Anwendung kann nicht automatisch virtuelle Rechner einschalten, die von CA ARCserve Central Host-Based VM Backup-Servern hinzugefügt wurden. Wenn Sie Richtlinien, die eine als "Virtuellen Rechner automatisch starten" festgelegte Wiederherstellungsmethode enthalten, auf Knoten bereitstellen, die durch Host-Based-VM-Backup geschützt sind, ändert Virtual Standby den Wert der Wiederherstellungsmethode auf "Virtuellen Rechner manuell starten".

Die Lösung für dieses Verhalten ist, den virtuellen Rechner mithilfe von CA ARCserve D2D oder CA ARCserve Central Protection Manager zu schützen.

Kapitel 6: Best Practices

Dieses Kapitel enthält folgende Themen:

Auswirkungen des Installationsprozesses auf das Betriebssystem (siehe Seite 217)
Funktionsweise der CA ARCserve Central Virtual Standby-Lizenzierung (siehe Seite 222)

Auswirkungen des Installationsprozesses auf das Betriebssystem

Durch den CA ARCserve Central Applications-Installationsprozess werden mithilfe des Installationsmoduls "Microsoft-Installationspaket" (MSI) verschiedene Komponenten des Windows-Betriebssystems aktualisiert. Mit den im MSI enthaltenen Komponenten kann CA ARCserve Central Applications benutzerdefinierte Aktionen zum Installieren, Aktualisieren oder Deinstallieren von CA ARCserve Central Applications durchführen.

In der folgenden Liste sind die benutzerdefinierten Aktionen und die betroffenen Komponenten aufgeführt.

Hinweis: Alle CA ARCserve Central Applications-MSI-Pakete rufen die in dieser Tabelle enthaltenen Komponenten auf, wenn Sie CA ARCserve Central Applications installieren und deinstallieren.

Komponente	Beschreibung
CallAllowInstall	Hiermit werden beim Installationsvorgang die Bedingungen überprüft, die einen Bezug zur aktuellen CA ARCserve Central Applications-Installation haben.
CallPreInstall	Hiermit können beim Installationsprozess MSI-Eigenschaften gelesen und geschrieben werden. Beispielsweise kann der CA ARCserve Central Applications-Installationspfad im MSI gelesen werden.
CallPostInstall	Hiermit können beim Installationsprozess verschiedene mit der Installation verbundene Aufgaben ausgeführt werden. Beispielsweise kann CA ARCserve Central Applications in der Windows-Registrierung registriert werden.
CallAllowUninstall	Hiermit werden beim Deinstallationsvorgang die Bedingungen überprüft, die einen Bezug zur aktuellen CA ARCserve Central Applications-Installation haben.

Komponente	Beschreibung
CallPreUninstall	Hiermit können beim Deinstallationsprozess verschiedene mit der Installation verbundene Aufgaben ausgeführt werden. Beispielsweise kann die Registrierung von CA ARCserve Central Applications in der Windows-Registrierung rückgängig gemacht werden.
CallPostUninstall	Hiermit werden beim Deinstallationsvorgang mehrere Aufgaben ausgeführt, nachdem die installierten Dateien deinstalliert wurden. Zum Beispiel können die restlichen Dateien entfernt werden.
ShowMsiLog	Zeigt die Protokolldatei von Windows Installer in Notepad an, wenn der Endbenutzer in den Dialogfeldern "Setup erfolgreich", "Setup fehlgeschlagen" oder "Setup unterbrochen" das Kontrollkästchen der Option "Protokolldatei von Windows Installer anzeigen" aktiviert und dann auf "Fertig stellen" klickt. (Dies funktioniert lediglich mit Windows Installer 4.0.)
ISPrint	Druckt die Inhalte eines Steuerelements mit scrollbarem Text auf einem Dialogfeld aus. Dies ist eine benutzerdefinierte Aktion der Windows-Installer-DLL. Die DLL-Datei heißt SetAllUsers.dll, und ihre Einsprungstelle ist PrintScrollableText.
CheckForProductUpdates	Verwendet FLEXnet Connect, um auf Produktaktualisierungen zu prüfen. Diese benutzerdefinierte Aktion startet eine ausführbare Datei mit dem Namen "Agent.exe" und gibt folgende Informationen weiter: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Verwendet FLEXnet Connect, um nach dem Neustart auf Produktaktualisierungen zu prüfen. Diese benutzerdefinierte Aktion startet eine ausführbare Datei mit dem Namen "Agent.exe" und gibt folgende Informationen weiter: /au[ProductCode] /EndOfInstall /Reboot

- **Aktualisierte Verzeichnisse:** Während des Installationsvorgangs werden CA ARCserve Central Applications-Dateien standardmäßig in den folgenden Verzeichnissen installiert und aktualisiert:

  `C:\Programme\CA\ARCserve Central Applications`

  Sie können CA ARCserve Central Applications im Standardinstallationsverzeichnis oder in einem alternativen Installationsverzeichnis installieren. Der Installationsprozess kopiert verschiedene Systemdateien ins folgende Verzeichnis:

  `C:\WINDOWS\SYSTEM32`

- **Aktualisierte Windows-Registrierungsschlüssel:** Der Installationsprozess aktualisiert die folgenden Windows-Registrierungsschlüssel:

  Standard-Registrierungsschlüssel:

  `HKLM\SOFTWARE\CA\CA ARCserve Central Applications`

  Basierend auf der aktuellen Konfiguration Ihres Systems werden beim Installationsprozess neue Registrierungsschlüssel erstellt und verschiedene weitere Registrierungsschlüssel geändert.

- **Installierte Anwendungen:** Beim Installationsprozess werden folgende Anwendungen auf Ihrem Computer installiert:
  - CA Licensing
  - Microsoft Visual C++ 2005 SP1 Redistributable
  - Microsoft Windows Installer 3.1 Redistributable (v2) Package
  - Java Runtime Environment (JRE) 1.6.0_16
  - Tomcat 6.0.32

Binärdateien mit unrichtigen Informationen zur Dateiversion

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA-Produkten und aus CA ARCserve Central Applications, die unrichtige Informationen zur Dateiversion enthalten. In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
UpdateData.exe	CA License
zlib1.dll	Zlib Compression Library

Binärdateien ohne eingebettetes Manifest

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA Technologies-Produkten und aus CA ARCserve Central Applications, die kein eingebettetes Manifest und kein Text-Manifest enthalten. In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
BaseLicInst.exe	CA License
UpdateData.exe	CA License

Binärname	Quelle
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

Binärdateien mit "Require Administrator"-Berechtigungen im Manifest

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA Technologies-Produkten und aus CA ARCserve Central Applications, die über die Berechtigungsebene "Administrator" oder "Highest Available" verfügen. Sie müssen sich mit einem Administratorkonto oder einem Konto mit den höchstmöglichen Berechtigungen anmelden, um verschiedene Dienste, Komponenten und Anwendungen von CA ARCserve Central Applications ausführen zu können. Die Binärdateien für diese Dienste, Komponenten und Anwendungen enthalten
CA ARCserve Central Applications-spezifische Funktionen, die für ein normales Benutzerkonto nicht verfügbar sind. Daher werden Sie von Windows aufgefordert, einen Vorgang zu bestätigen, indem Sie Ihr Kennwort angeben oder ein Konto mit Administratorrechten verwenden, um den Vorgang auszuführen.

- **Administratorrechte** - Das Administratorprofil sowie Konten mit Administratorrechten verfügen über Schreib-, Lese- und Ausführungsberechtigungen für alle Windows- und Systemressourcen. Wenn Sie über keine Administratorrechte verfügen, werden Sie aufgefordert, den Benutzernamen und das Kennwort eines Administrators einzugeben, um fortfahren zu können.
- **Höchstmögliche Berechtigungen** - Bei einem Konto mit den höchst möglichen Berechtigungen handelt es sich um ein normales Benutzerkonto oder Poweruser-Konto, mit dem Administratorrechte genutzt werden können.

In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications

Binärname	Quelle
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Funktionsweise der CA ARCserve Central Virtual Standby-Lizenzierung

CA ARCserve Central Virtual Standby enthält folgende Lizenzen:

- CA ARCserve Central Virtual Standby-Physical
- CA ARCserve Central Virtual Standby-VMware
- CA ARCserve Central Virtual Standby-Hyper-V

Alle Lizenzen sind anzahlbasiert. CA ARCserve Central Virtual Standby überprüft und erteilt Lizenzen für CA ARCserve D2D-Knoten, die auf folgenden Kriterien basieren:

- CA ARCserve Central Virtual Standby wendet CA ARCserve Central Virtual Standby-Physical-Lizenzen auf alle CA ARCserve D2D-Knoten an, die Sie nach Namen/IP-Adresse hinzufügen oder die Sie aus einer Datei importieren. CA ARCserve Central Virtual Standby erteilt CA ARCserve Central Virtual Standby-Physical-Lizenzen für Knoten, nachdem Sie eine Richtlinie auf die Knoten angewendet und den virtuellen Konvertierungsprozess gestartet haben.

  Hinweis: Dies ist das Standardverhalten für CA ARCserve Central Virtual Standby-Lizenzierung.

- CA ARCserve Central Virtual Standby wendet CA ARCserve Central Virtual Standby-VMware-Lizenzen auf alle CA ARCserve D2D-Knoten an, die Sie nach Namen/IP-Adresse hinzufügen, die Sie aus einer Datei importieren und die virtuelle VMware-Rechner sind, die sich auf ESX Server-Systeme oder vCenter Server-Systeme befinden. Bevor CA ARCserve Central Virtual Standby die CA ARCserve Central Virtual Standby-VMware-Lizenzen auf die Knoten anwenden kann, müssen Sie allerdings die Knoten mit einem bestimmten ESX Server-System oder vCenter Server-System verbinden.

  Hinweis: Weitere Informationen finden Sie unter Geben Sie das ESX Server- oder vCenter Server-System für VMware-basierte Knoten an (siehe Seite 30).

  CA ARCserve Central Virtual Standby erteilt die CA ARCserve Central Virtual Standby-VMware-Lizenzen für jedes ESX Server-System, nachdem Sie eine Richtlinie auf die Knoten angewendet und den virtuellen Konvertierungsprozess gestartet haben.

- CA ARCserve Central Virtual Standby wendet
  CA ARCserve Central Virtual Standby-VMware-Lizenzen auf alle virtuellen Rechnerknoten an, die Sie aus einem
  CA ARCserve Central Host-Based VM Backup-System importieren.
  CA ARCserve Central Virtual Standby erteilt die
  CA ARCserve Central Virtual Standby-VMware-Lizenzen für virtuelle Rechnerknoten, nachdem Sie eine Richtlinie auf die Knoten angewendet und den virtuellen Konvertierungsprozess gestartet haben.
- CA ARCserve Central Virtual Standby wendet
  CA ARCserve Central Virtual Standby-Hyper-V-Lizenzen auf alle
  CA ARCserve D2D-Knoten an, die Sie nach Namen/IP-Adresse hinzufügen, aus einer Datei importieren und die sich auf einem Hyper-V-Hypervisor befinden.
  CA ARCserve Central Virtual Standby erkennt, dass der Hyper-V-Server vorhanden ist, wenn Sie Knoten nach Namen/IP-Adresse hinzufügen oder Knoten aus einer Datei importieren. CA ARCserve Central Virtual Standby erteilt
  CA ARCserve Central Virtual Standby-Hyper-V-Lizenzen für
  CA ARCserve D2D-Knoten nachdem Sie Knoten nach Namen/IP-Adresse hinzufügen oder Knoten aus einer Datei importieren.

Zählmethode

Folgende Tabelle beschreibt die Anzahl der
CA ARCserve Central Virtual Standby-Lizenzen, die für ein bestimmtes Szenario erforderlich sind.

Typ des D2D-Knoten	Erforderliche Lizenz	Zählmethode
Physischer Knoten	CA ARCserve Central Virtual Standby -Physical	Eine Lizenz für jeden Knoten
Virtueller VMware-Rechner	CA ARCserve Central Virtual Standby -VMware	Eine Lizenz für jedes ESX/vCenter Server-System
Virtueller Hyper-V-Rechner	CA ARCserve Central Virtual Standby -Hyper-V	Eine Lizenz für jedes Hyper-V-System

Beispiele

- CA ARCserve Central Virtual Standby schützt fünf physische CA ARCserve D2D-Knoten. Es sind fünf Lizenzen für CA ARCserve Central Virtual Standby-Physical erforderlich.
- CA ARCserve Central Virtual Standby schützt drei virtuelle VMware-Rechner, die sich auf einem ESX Server-System befinden. Es ist eine Lizenz für CA ARCserve Central Virtual Standby-VMware erforderlich.
- CA ARCserve Central Virtual Standby schützt 100 virtuelle VMware-Rechner, die auf zehn ESX Server-Systemen verteilt sind. Es sind zehn Lizenzen für CA ARCserve Central Virtual Standby erforderlich.
- CA ARCserve Central Virtual Standby schützt 20 virtuelle Hyper-V-Rechner, die auf fünf Hyper-V-Systemen verteilt sind. Es sind fünf Lizenzen für CA ARCserve Central Virtual Standby-Hyper-V erforderlich.
- CA ARCserve Central Virtual Standby schützt drei virtuelle Hyper-V-Rechner, die sich auf einem Hyper-V-System befinden, und drei virtuelle VMware-Rechner, die sich auf einem ESX Server-System befinden. Es ist eine Lizenz für CA ARCserve Central Virtual Standby-VMware und eine Lizenz für CA ARCserve Central Virtual Standby-Hyper-V erforderlich.
- CA ARCserve Central Virtual Standby schützt fünf virtuelle VMware-Rechner, die aus CA ARCserve Central Host-Based VM Backup importiert wurden und sich auf einem ESX Server-System befinden. Es ist eine Lizenz für CA ARCserve Central Virtual Standby-VMware erforderlich.

Terminologieglossar

Heartbeat-Signal

Ein Heartbeat-Signal ist ein elektronisches Signal, das Quellknoten zu Überwachungsservern senden, um den Status des Knotens zu überwachen.

HOTADD-Transportmodus

Der Hotadd-Transportmodus ist eine Methode zum Datentransport, mit der Sie mit SCSI-Datenträgern konfigurierte virtuelle Rechner sichern können. Weitere Informationen finden Sie im "Virtual Disk API Programming Guide" auf der VMware-Website.

Knoten

Ein Knoten ist ein physischer oder virtueller Rechner, der über einen oder mehrere CA ARCserve Central Applications verwaltet wird.

Knotengruppe

Eine Knotengruppe ist eine Methode, bei der alle Knoten, die über eine oder mehrere CA ARCserve Central Applications verwaltet werden, organisiert werden können, wie beispielsweise nach Zweck, Betriebssystem oder nach installierten Anwendungen.

NBDSSL-Transportmodus

Der Transportmodus für Network Block Device Secure Sockets Layer (NBDSSL) verwendet das NFC-Protokoll (Network File Copy) zur Kommunikation. NBDSSL-Übertragungen verschlüsseln Daten mithilfe des TCP/IP-Kommunikationsnetzwerks.

NBD-Transportmodus

Der NBD-Transportmodus (Network Block Device), auch LAN-Transportmodus genannt, verwendet das NFC-Protokoll (Network File Copy) zum Kommunizieren. Verschiedene VDDK- und VCB-Vorgänge verwenden eine Verbindung für jeden virtuellen Datenträger, auf den bei der Verwendung von NBD auf jedem ESX-/ESXi-Server-Host zugegriffen wird.

Richtlinie

Eine Richtlinie ist eine Gruppe von Spezifikationen, um einen Knotens in einer oder mehreren CA ARCserve Central Applications zu schützen.

SAN-Transportmodus

Der SAN-Transportmodus (Storage Area Network) ermöglicht es Ihnen, Sicherungsdaten von Proxy-Systemen, die mit SAN verbunden sind, mithilfe von FibreChannel-Kommunikation in Speichergeräte zu übertragen.

Überwachungsserver

Ein Überwachungsserver ist ein Server, der den Status von Quellservern in CA ARCserve Central Virtual Standby-Umgebungen überprüft.

Virtuelle Konvertierung

Virtuelle Konvertierung ist der Prozess, bei dem CA ARCserve Central Virtual Standby CA ARCserve D2D-Wiederherstellungspunkte von Quellknoten in Datendateien virtueller Rechner konvertiert, die als Wiederherstellungspunkt-Snapshots bezeichnet werden.

Wiederherstellungspunkt

Ein Wiederherstellungspunkt ist ein Sicherungs-Image, das übergeordnete und die ältesten untergeordneten Blöcke umfasst. Untergeordnete Sicherungen werden mit der übergeordneten Sicherung zusammengeführt, um neue Wiederherstellungspunkt-Images zu erstellen, sodass der angegebene Wert immer verwaltet wird.

Wiederherstellungspunkt-Snapshot

Ein Wiederherstellungspunkt-Snapshot ist eine VMware Virtual Disk (VMDK) oder Microsoft Virtual Hard Disk-Datei (VHD), die CA ARCserve Central Virtual Standby aus CA ARCserve D2D-Wiederherstellungspunkten erstellt. Mit CA ARCserve Central Virtual Standby können Sie virtuelle Rechner mithilfe von Wiederherstellungspunkt-Snapshots einschalten, wenn die Quellserver in Ihrer Produktionsumgebung, die CA ARCserve D2D ausführen, fehlschlagen.

Index

A

Aktualisieren von Knoten - 51
Aktualisieren von Knoten und Richtlinien nach einer Änderung des Hostnamens des CA ARCserve Central Applications-Servers - 56
Ändern des Administratorkontos - 74
Ändern des Server-Kommunikationsprotokolls - 178
Ändern von Knotengruppen - 57
Änderungen in der Dokumentation - 4
Anmelden an Überwachungsservern - 44
Anmelden bei CA ARCserve D2D-Knoten - 43
Anmeldung bei CA ARCserve Central Virtual Standby - 27
Anzeigen der Liste der Wiederherstellungspunkt-Snapshots - 83
Anzeigen der Virtual Standby-Einstellungen für Quellserver - 82
Anzeigen von - 80
Anzeigen von Aktivitätsprotokolldaten über Jobs - 94
Anzeigen von Informationen über zu CA ARCserve D2D-Knoten zugewiesenen Richtlinien - 100
Anzeigen von Protokollen - 76
Anzeigen von Statusinformationen zu Virtual Standby-Jobs vom Virtual Standby-Server aus - 97
Anzeigen von Statusinformationen zu Virtual Standby-Jobs von Knoten aus - 98
Aufgaben zur Verwaltung von Knotengruppen - 56
Aufgaben zur Wartung von Knoten - 45
Auswirkungen des Installationsprozesses auf das Betriebssystem - 217

B

Bearbeiten oder Kopieren von Richtlinien - 60
Beheben von Problemen beim Laden von Seiten - 186
Bei der Anmeldung in CA ARCserve D2D-Knoten und -Überwachungsserver werden Webseiten nicht richtig geladen - 187
Bei der Verwendung einer japanischen Tastatur können in Filterfeldern keine Sternchen und Unterstriche als ein Platzhalter verwendet werden - 216
Bei Sicherungen und Wiederherstellungen im Hotadd-Transportmodus werden Datenträger nicht geladen - 210
Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt. - 195
Beim Hinzufügen von Knoten werden ungültige Anmeldeinformationen angezeigt. - 196
Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist. - 182
Bereitstellen von Richtlinien - 40
Best Practices - 217
Binärdateien mit - 220
Binärdateien mit unrichtigen Informationen zur Dateiversion - 219
Binärdateien ohne eingebettetes Manifest - 219

C

CA ARCserve Central Applications-Bookshelf - 14
CA ARCserve Central Virtual Standby automatisch deinstallieren - 23
CA ARCserve Central Virtual Standby automatisch installieren - 20
CA ARCserve Central Virtual Standby kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen. - 194
CA ARCserve Central Virtual Standby-Überwachungs-Aufgaben - 83
CA ARCserve D2D-Webservice schlägt auf CA ARCserve D2D-Knoten fehl - 189
CA Kontaktieren - 3
CA Technologies-Produktreferenzen - 3

D

Deinstallieren von CA ARCserve Central Virtual Standby - 20
Der CA ARCserve D2D-Webservice wird nur langsam ausgeführt. - 192
Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet - 212

Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer 8 und 9 nicht ordnungsgemäß geöffnet - 215

E

Einführung - 11
Einführung in CA ARCserve Central Virtual Standby - 11
Einschalten von virtuellen Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots - 90
Einschalten von virtuellen Virtual Standby-Rechnern über VMware vSphere Client - 93
Einschalten von virtueller Virtual Standby-Rechner über den Hyper-V-Manager - 91
Einstellungen von Virtual Standby - 101
Erforderliche Installationsaufgaben - 15
Erste Schritte mit CA ARCserve Central Virtual Standby - 25
Erstellen von Richtlinien - 32

F

Fehler - 201
Fehler wegen verweigerten Zugriffs beim Hinzufügen eines Knotens nach IP/Namen - 198
Fehlerbehebung in CA ARCserve Central Virtual Standby - 181
Fehlernummern der Fehlerbehebung - 211
Filtern von Knotengruppen - 59
Freigeben von Lizenzen von Knoten - 53
Funktionsweise der CA ARCserve Central Virtual Standby-Lizenzierung - 222
Funktionsweise von CA ARCserve Central Virtual Standby - 12

G

Geben Sie das ESX Server- oder vCenter Server-System für VMware-basierte Knoten an - 30

H

Heartbeat-Signal - 225
Hinzufügen von Knoten nach IP-Adresse oder Knotennamen - 28
Hinzufügen von Knoten von CA ARCserve Central Host-Based VM Backup-Servern - 48
Hinzufügen von Knotengruppen - 29
HOTADD-Transportmodus - 225

I

Importieren von Knoten aus einer Datei - 46
Installation von CA ARCserve Central Virtual Standby - 15, 18
Installationshinweise - 17

K

Knoten - 225
Knoten werden nach einer Namensänderung nicht mehr im Bildschirm - 200
Knotengruppe - 225
Konfigurationsaufgaben der Anwendung - 69
Konfigurieren automatischer Updates - 70
Konfigurieren der E-Mail-Einstellungen - 69
Konfigurieren von Voreinstellungen für Social Networking - 73

L

Leere Webseiten oder JavaScript-Fehler treten auf - 184
Links zur Navigationsleiste hinzufügen - 77
Löschen von Aktivitätsprotokolldatensätzen - 96
Löschen von Knoten - 52
Löschen von Knotengruppen - 58
Löschen von Richtlinien - 68

M

Meldungen zu ungültigen Anmeldeinformationen unter Windows XP - 197

N

NBDSSL-Transportmodus - 225
NBD-Transportmodus - 225

P

Proxy-Einstellungen konfigurieren - 72

R

Richtlinie - 225

S

SAN-Transportmodus - 225
Sicherungs- und Wiederherstellungsjobs verwenden den SAN-Transportmodus nicht - 208
So schützen Sie virtuelle Virtual Standby-Rechner - 105
So verwenden Sie den Bildschirm - 78
So verwenden Sie die Serverliste - 79
Startseite von Virtual Standby - 78
Statusüberwachung für Virtual Standby - 99
Stellen Sie sicher, dass der CA ARCserve Central Virtual Standby-Server mit den Knoten kommunizieren kann. - 26
Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift. - 188

U

Überwachen des Status von virtuellen Konvertierungsjobs - 81
Überwachen von Knoten über den Überwachungsserver beenden - 55
Überwachungsserver - 225
Unterbrechen und Wiederaufnehmen von Heartbeat-Signalen des Virtual Standby-Servers - 84
Unterbrechen und Wiederaufnehmen von Heartbeat-Signalen von den Knoten aus - 86
Unterbrechen und Wiederaufnehmen von Virtual Standby-Jobs vom Virtual Standby-Server aus - 87
Unterbrechen und Wiederaufnehmen von Virtual Standby-Jobs von den Knoten aus - 88

V

Verwaltungsaufgaben zu Virtual Standby-Richtlinien - 59
Verwenden von CA ARCserve Central Virtual Standby - 43
Virtual Standby-Jobs an Hyper-V-Systeme schlagen fehl - 202
Virtual Standby-Jobs enden Mit Warnmeldungen zu fehlenden Sitzungen - 207
Virtual Standby-Jobs im Hotadd-Transportmodus schlagen fehl - 205
Virtual Standby-Jobs schlagen aufgrund interner Fehler fehl - 202
Virtuelle Konvertierung - 226
Virtuelle Rechner nicht automatisch eingeschaltet - 216

W

Wiederherstellen von Daten aus CA ARCserve D2D-Dateikopien - 112
Wiederherstellen von Daten aus CA ARCserve D2D-Wiederherstellungspunkten - 107
Wiederherstellen von Daten mithilfe von - 117
Wiederherstellen von Microsoft Exchange-E-Mail-Nachrichten - 169
Wiederherstellen von Quellservern mithilfe von Bare-Metal-Recovery - 122
Wiederherstellen von Quellservern mithilfe von CA ARCserve D2D-Sicherungsdaten - 124
Wiederherstellen von Quellservern mithilfe von Daten aus Hyper-V-basierten virtuellen Virtual Standby-Rechnern - 139
Wiederherstellen von Quellservern mithilfe von Daten aus VMware-basierten virtuellen Virtual Standby-Rechnern - 153
Wiederherstellungspunkt - 226
Wiederherstellungspunkt-Snapshot - 226

Z

Zuweisen von Knoten zu Richtlinien - 39
Zuweisung von Knoten zu Richtlinien aufheben - 67